

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2024-10-14.1 | 14 октября 2024 года

TLP: WHITE



Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-38229	Microsoft .NET and Visual Studio	Сетевой	ACE	2024-10-09	✓
2	Высокая	CVE-2024-43576	Microsoft Office	Локальный	ACE	2024-10-09	✓
3	Высокая	CVE-2024-43485	Microsoft .NET and Visual Studio	Сетевой	DoS	2024-10-09	✓
4	Высокая	CVE-2024-43616	Microsoft Office	Локальный	ACE	2024-10-09	✓
5	Высокая	CVE-2024-38212	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
6	Высокая	CVE-2024-43593	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
7	Высокая	CVE-2024-43589	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
8	Высокая	CVE-2024-45142	Adobe Substance 3D Stager	Локальный	ACE	2024-10-08	✓
9	Высокая	CVE-2024-43611	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
10	Высокая	CVE-2024-45152	Adobe Substance 3D Stager	Локальный	ACE	2024-10-08	✓
11	Высокая	CVE-2024-43592	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
12	Высокая	CVE-2024-45144	Adobe Substance 3D Stager	Локальный	ACE	2024-10-08	✓

13	Высокая	CVE-2024-38261	Microsoft Windows Routing and Remote Access Service (RRAS)	Локальный	ACE	2024-10-08	✓
14	Высокая	CVE-2024-45143	Adobe Substance 3D Stager	Локальный	ACE	2024-10-08	✓
15	Высокая	CVE-2024-43607	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
16	Высокая	CVE-2024-45141	Adobe Substance 3D Stager	Локальный	ACE	2024-10-08	✓
17	Высокая	CVE-2024-43608	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
18	Высокая	CVE-2024-45140	Adobe Substance 3D Stager	Локальный	ACE	2024-10-08	✓
19	Высокая	CVE-2024-43453	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
20	Высокая	CVE-2024-45139	Adobe Substance 3D Stager	Локальный	ACE	2024-10-08	✓
21	Высокая	CVE-2024-43564	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
22	Высокая	CVE-2024-38265	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
23	Высокая	CVE-2024-45138	Adobe Substance 3D Stager	Локальный	ACE	2024-10-08	✓
24	Высокая	CVE-2024-43549	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-10-08	✓
25	Высокая	CVE-2024-43599	Microsoft Remote Desktop Client	Сетевой	ACE	2024-10-08	✓

26	Высокая	CVE-2024-43533	Microsoft Remote Desktop Client	Сетевой	ACE	2024-10-08	✓
27	Высокая	CVE-2024-43519	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-10-09	✓
28	Высокая	CVE-2024-43488	Microsoft Visual Studio Code extension for Arduino	Сетевой	ACE	2024-10-09	✓
29	Критическая	CVE-2024-43468	Microsoft Configuration Manager	Сетевой	ACE	2024-10-09	✓
30	Высокая	CVE-2024-43574	Microsoft Speech Application Programming Interface (SAPI)	Сетевой	ACE	2024-10-09	✓
31	Высокая	CVE-2024-43504	Microsoft Excel	Локальный	ACE	2024-10-09	✓
32	Высокая	CVE-2024-43582	Microsoft Remote Desktop Protocol Server	Сетевой	ACE	2024-10-09	✓
33	Высокая	CVE-2024-43517	Microsoft ActiveX Data Objects	Сетевой	ACE	2024-10-09	✓
34	Высокая	CVE-2024-43497	Microsoft DeepSpeed	Локальный	ACE	2024-10-08	✓
35	Высокая	CVE-2024-43518	Microsoft Windows Telephony Server	Сетевой	ACE	2024-10-08	✓
36	Высокая	CVE-2024-43505	Microsoft Office Visio	Локальный	ACE	2024-10-08	✓
37	Высокая	CVE-2024-43572	Microsoft Management Console	Локальный	ACE	2024-10-08	✓
38	Высокая	CVE-2023-6874	Siemens Sentron Powercenter 1000 with 3RV2921-5M accessory	Сетевой	DoS	2024-10-11	✗
39	Высокая	CVE-2024-47562	Siemens SINEC Security Monitor	Локальный	ACE	2024-10-09	✓

40	Критическая	CVE-2024-47553	Siemens SINEC Security Monitor	Сетевой	ACE	2024-10-09	✓
41	Высокая	CVE-2024-39515	Junos OS Evolved and Juniper Junos OS	Сетевой	DoS	2024-10-11	✓
42	Высокая	CVE-2024-47504	Juniper Junos OS	Сетевой	DoS	2024-10-11	✓
43	Высокая	CVE-2024-39516	Junos OS Evolved and Juniper Junos OS	Сетевой	DoS	2024-10-11	✓
44	Критическая	CVE-2024-9465	Palo Alto Networks Expedition	Сетевой	ACE	2024-10-11	✓
45	Критическая	CVE-2024-9464	Palo Alto Networks Expedition	Сетевой	ACE	2024-10-11	✓
46	Критическая	CVE-2024-9463	Palo Alto Networks Expedition	Сетевой	ACE	2024-10-11	✓
47	Высокая	CVE-2024-41902	Siemens JT2Go	Локальный	ACE	2024-10-10	✓
48	Высокая	CVE-2024-47046	Siemens Simcenter Nastran	Локальный	ACE	2024-10-10	✓
49	Высокая	CVE-2024-41981	Siemens Simcenter Nastran	Локальный	ACE	2024-10-10	✓
50	Критическая	None	wkhtmltopdf module for Drupal	Сетевой	OSI	2024-10-10	✗
51	Критическая	CVE-2024-39563	Junos Space	Сетевой	ACE	2024-10-10	✓
52	Высокая	CVE-2024-47490	Junos OS Evolved	Сетевой	DoS	2024-10-10	✓
53	Высокая	CVE-2024-9680	Mozilla Firefox , Firefox ESR и Thunderbird	Сетевой	ACE	2024-10-09	✓
54	Высокая	CVE-2024-45475	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-10-09	✓

55	Высокая	CVE-2024-45474	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-10-09	✓
56	Высокая	CVE-2024-45473	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-10-09	✓
57	Высокая	CVE-2024-45472	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-10-09	✓
58	Высокая	CVE-2024-45471	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-10-09	✓
59	Высокая	CVE-2024-45470	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-10-09	✓
60	Высокая	CVE-2024-45469	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-10-09	✓
61	Высокая	CVE-2024-45468	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-10-09	✓
62	Высокая	CVE-2024-45467	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-10-09	✓
63	Высокая	CVE-2024-45466	Siemens Tecnomatix Plant Simulation	Локальный	OSI	2024-10-09	✓
64	Высокая	CVE-2024-45465	Siemens Tecnomatix Plant Simulation	Локальный	OSI	2024-10-09	✓
65	Высокая	CVE-2024-45464	Siemens Tecnomatix Plant Simulation	Локальный	OSI	2024-10-09	✓
66	Высокая	CVE-2024-45463	Siemens Tecnomatix Plant Simulation	Локальный	OSI	2024-10-09	✓
67	Высокая	CVE-2024-45150	Adobe Dimension	Локальный	ACE	2024-10-09	✓
68	Высокая	CVE-2024-45146	Adobe Dimension	Локальный	ACE	2024-10-09	✓
69	Высокая	CVE-2024-45137	Adobe InDesign	Локальный	ACE	2024-10-09	✓

70	Высокая	CVE-2024-47425	Adobe Framemaker	Локальный	ACE	2024-10-09	✓
71	Высокая	CVE-2024-47424	Adobe Framemaker	Локальный	ACE	2024-10-09	✓
72	Высокая	CVE-2024-47423	Adobe Framemaker	Локальный	ACE	2024-10-09	✓
73	Высокая	CVE-2024-47422	Adobe Framemaker	Локальный	ACE	2024-10-09	✓
74	Высокая	CVE-2024-47421	Adobe Framemaker	Локальный	ACE	2024-10-09	✓
75	Высокая	CVE-2024-47418	Adobe Animate	Локальный	ACE	2024-10-09	✓
76	Высокая	CVE-2024-47417	Adobe Animate	Локальный	ACE	2024-10-09	✓
77	Высокая	CVE-2024-47416	Adobe Animate	Локальный	ACE	2024-10-09	✓
78	Высокая	CVE-2024-47415	Adobe Animate	Локальный	ACE	2024-10-09	✓
79	Высокая	CVE-2024-45136	Adobe InCopy	Локальный	ACE	2024-10-09	✓
80	Высокая	CVE-2024-47414	Adobe Animate	Локальный	ACE	2024-10-09	✓
81	Высокая	CVE-2024-47413	Adobe Animate	Локальный	ACE	2024-10-09	✓
82	Высокая	CVE-2024-47412	Adobe Animate	Локальный	ACE	2024-10-09	✓
83	Высокая	CVE-2024-47411	Adobe Animate	Локальный	ACE	2024-10-09	✓
84	Высокая	CVE-2024-47410	Adobe Animate	Локальный	ACE	2024-10-09	✓

85	Высокая	CVE-2024-9603	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-10-09	✓
86	Высокая	CVE-2024-9602	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-10-09	✓
87	Высокая	CVE-2024-42417	Delta Electronics DIAEnergie	Сетевой	ACE	2024-10-07	✓
88	Критическая	CVE-2024-43699	Delta Electronics DIAEnergie	Сетевой	ACE	2024-10-07	✓
89	Высокая	CVE-2024-47807	Jenkins OpenId Connect Authentication plugin	Сетевой	SB	2024-10-07	✓
90	Высокая	CVE-2024-47806	Jenkins OpenId Connect Authentication plugin	Сетевой	SB	2024-10-07	✓
91	Высокая	CVE-2024-36474	GNOME libgsf	Локальный	ACE	2024-10-07	✓
92	Высокая	CVE-2024-42415	GNOME libgsf	Локальный	ACE	2024-10-07	✓
93	Критическая	CVE-2024-20510	Cisco IOS XE Software	Смежная сеть	SB	2024-09-26	✓

Краткое описание: Выполнение произвольного кода в Microsoft .NET and Visual Studio

Идентификатор уязвимости: CVE-2024-38229

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Visual Studio: 2022 версии 17.6 и 2022 версии 17.11
.NET: версии 8.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

1

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38229>

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2024-43576

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Microsoft Office LTSC: 2024
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

2 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43576>

Краткое описание: Отказ в обслуживании в Microsoft .NET and Visual Studio

Идентификатор уязвимости: CVE-2024-43485

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Visual Studio: 2022 версии 17.6 и 2022 версии 17.11
.NET: с версии 6.0.0 по 8.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

3 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43485>

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2024-43616

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43616>

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-38212
BDU:2024-07934

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

- 5 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38212>
- <https://bdu.fstec.ru/vul/2024-07934>

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-43593
BDU:2024-07952

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

6 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43593>
- <https://bdu.fstec.ru/vul/2024-07952>

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-43589
BDU:2024-07956

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

- 7 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43589>
- <https://bdu.fstec.ru/vul/2024-07956>

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2024-45142

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Substance 3D Stager: с версии 2.0.0 по 3.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

8 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-81.html

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-43611
BDU:2024-07951

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

- 9 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43611>
- <https://bdu.fstec.ru/vul/2024-07951>

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2024-45152

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: с версии 2.0.0 по 3.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

10 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-81.html

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-43592
BDU:2024-07950

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

11

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43592>
- <https://bdu.fstec.ru/vul/2024-07950>

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2024-45144

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: с версии 2.0.0 по 3.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

12 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-81.html

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-38261
BDU:2024-07966

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

13 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38261>
- <https://bdu.fstec.ru/vul/2024-07966>

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2024-45143

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Substance 3D Stager: с версии 2.0.0 по 3.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

14 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-81.html

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-43607
BDU:2024-07953

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

15 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43607>
- <https://bdu.fstec.ru/vul/2024-07953>

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2024-45141

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: с версии 2.0.0 по 3.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

16 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-81.html

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-43608
BDU:2024-07955

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

17 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43608>
- <https://bdu.fstec.ru/vul/2024-07955>

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2024-45140

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: с версии 2.0.0 по 3.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

18 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-81.html

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-43453
BDU:2024-07967

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

19 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43453>
- <https://bdu.fstec.ru/vul/2024-07967>

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2024-45139

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Substance 3D Stager: с версии 2.0.0 по 3.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

20 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-81.html

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-43564

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows Server: до 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

21

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43564>

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-38265
BDU:2024-07972

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows Server: до 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

22 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38265>
- <https://bdu.fstec.ru/vul/2024-07972>

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2024-45138

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Substance 3D Stager: с версии 2.0.0 по 3.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

23

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-81.html
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1331/>

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-43549

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

24 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43549>

Краткое описание: Выполнение произвольного кода в Microsoft Remote Desktop Client

Идентификатор уязвимости: CVE-2024-43599
BDU:2024-07933

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до версии 11 24H2 10.0.26100.2033
Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

25 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43599>
- <https://bdu.fstec.ru/vul/2024-07933>

Краткое описание: Выполнение произвольного кода в Microsoft Remote Desktop Client

Идентификатор уязвимости: CVE-2024-43533
BDU:2024-07932

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189
Windows: до версии 11 24H2 10.0.26100.2033

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

26 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43533>
- <https://bdu.fstec.ru/vul/2024-07932>

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-43519

Идентификатор программной ошибки: CWE-197 Ошибка числовых усечений

Уязвимый продукт: Windows: до версии 11 24H2 10.0.26100.2033
Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносной базе данных SQL.

Последствия эксплуатации: Выполнение произвольного кода

27 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43519>

Краткое описание: Выполнение произвольного кода в Microsoft Visual Studio Code extension for Arduino

Идентификатор уязвимости: CVE-2024-43488

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: Visual Studio Code: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Выполнение произвольного кода

28 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43488>

Краткое описание: Выполнение произвольного кода в Microsoft Configuration Manager

Идентификатор уязвимости: CVE-2024-43468
BDU:2024-07944

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Configuration Manager: с версии 2303 по 2403

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

29 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43468>
- <https://bdu.fstec.ru/vul/2024-07944>

Краткое описание: Выполнение произвольного кода в Microsoft Speech Application Programming Interface (SAPI)

Идентификатор уязвимости: CVE-2024-43574

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows Server: до версии 2022 23H2 10.0.25398.1189
Windows: до версии 11 24H2 10.0.26100.2033

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

30 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43574>

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2024-43504

BDU:2024-07981

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Office: 2019

Microsoft Excel: 2016

Microsoft Office LTSC: 2021 - 2024

Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

31

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43504>
- <https://bdu.fstec.ru/vul/2024-07981>

Краткое описание: Выполнение произвольного кода в Microsoft Remote Desktop Protocol Server

Идентификатор уязвимости: CVE-2024-43582
BDU:2024-07936

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до версии 11 24H2 10.0.26100.2033
Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

32 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43582>
- <https://bdu.fstec.ru/vul/2024-07936>

Краткое описание: Выполнение произвольного кода в Microsoft ActiveX Data Objects

Идентификатор уязвимости: CVE-2024-43517
BDU:2024-07975

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows: до версии 11 24H2 10.0.26100.2033
Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

33 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43517>
- <https://bdu.fstec.ru/vul/2024-07975>

Краткое описание: Выполнение произвольного кода в Microsoft DeepSpeed

Идентификатор уязвимости: CVE-2024-43497

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: DeepSpeed: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

34 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43497>

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Server

Идентификатор уязвимости: CVE-2024-43518
BDU:2024-07973

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows: до версии 11 24H2 10.0.26100.2033
Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

35 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43518>
- <https://bdu.fstec.ru/vul/2024-07973>

Краткое описание: Выполнение произвольного кода в Microsoft Office Visio

Идентификатор уязвимости: CVE-2024-43505
BDU:2024-07941

Идентификатор программной ошибки: CWE-357 Недостаточно очевидное предупреждение об опасных операциях

Уязвимый продукт: Microsoft Office: 2019
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Office LTSC: 2021 - 2024

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43505>
- <https://bdu.fstec.ru/vul/2024-07941>

Краткое описание: Выполнение произвольного кода в Microsoft Management Console

Идентификатор уязвимости: CVE-2024-43572
BDU:2024-07877

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: до версии 11 24H2 10.0.26100.2033
Windows Server: до версии 2022 23H2 10.0.25398.1189

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

37 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-08 / 2024-10-08

Ссылки на источник:

- <http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43572>
- <https://bdu.fstec.ru/vul/2024-07877>

Краткое описание: Отказ в обслуживании в Siemens Sentron Powercenter 1000 with 3RV2921-5M accessory

Идентификатор уязвимости: CVE-2023-6874

Идентификатор программной ошибки: CWE-754 Некорректная проверка наличия нестандартных условий или исключений

Уязвимый продукт: SENTRON Powercenter 1000: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

38 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-11 / 2024-10-11

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-340240.txt>

Краткое описание: Выполнение произвольного кода в Siemens SINEC Security Monitor

Идентификатор уязвимости: CVE-2024-47562

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: Siemens SINEC Security Monitor: до 4.9.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

39 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/html/ssa-430425.html>

Краткое описание: Выполнение произвольного кода в Siemens SINEC Security Monitor

Идентификатор уязвимости: CVE-2024-47553

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: Siemens SINEC Security Monitor: до 4.9.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

40 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/html/ssa-430425.html>

Краткое описание: Отказ в обслуживании в Junos OS Evolved and Juniper Junos OS

Идентификатор уязвимости: CVE-2024-39515

Идентификатор программной ошибки: CWE-1288 Некорректная проверка согласованности входных данных

Уязвимый продукт: Junos OS Evolved: 21.4R1-EVO - 22.2R3-S4-EVO
Juniper Junos OS: 21.4R1 - 22.2R3-S4.11

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

41

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-11 / 2024-10-11

Ссылки на источник:

- <http://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-With-BGP-traceoptions-enabled-receipt-of-specially-crafted-BGP-update-causes-RPD-crash-CVE-2024-39515>

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2024-47504

Идентификатор программной ошибки: CWE-1287 Некорректная проверка заданного типа входных данных

Уязвимый продукт: Juniper Junos OS: 22.2R1 - 22.2R3-S4.11

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

42

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-11 / 2024-10-11

Ссылки на источник:

- <http://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-JunOS-SRX5000-Series-Receipt-of-a-specific-malformed-packet-will-cause-a-flowd-crash-CVE-2024-47504>

Краткое описание: Отказ в обслуживании в Junos OS Evolved and Juniper Junos OS

Идентификатор уязвимости: CVE-2024-39516

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Junos OS Evolved: 21.4R1-EVO - 22.2R3-S4-EVO
Juniper Junos OS: 21.4R1 - 22.2R3-S4.11

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

43

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-11 / 2024-10-11

Ссылки на источник:

- <http://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Junos-OS-and-Junos-OS-Evolved-Receipt-of-a-specifically-malformed-BGP-packet-causes-RPD-crash-when-segment-routing-is-enabled-CVE-2024-39516>

Краткое описание: Выполнение произвольного кода в Palo Alto Networks Expedition

Идентификатор уязвимости: CVE-2024-9465
BDU:2024-07930

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Expedition: 1.0.91 - 1.2.95

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

44 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-11 / 2024-10-11

Ссылки на источник:

- <http://security.paloaltonetworks.com/PAN-SA-2024-0010>
- <https://bdu.fstec.ru/vul/2024-07930>

Краткое описание: Выполнение произвольного кода в Palo Alto Networks Expedition

Идентификатор уязвимости: CVE-2024-9464

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: Expedition: 1.0.91 - 1.2.95

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

45 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-11 / 2024-10-11

Ссылки на источник:

- <http://security.paloaltonetworks.com/PAN-SA-2024-0010>

Краткое описание: Выполнение произвольного кода в Palo Alto Networks Expedition

Идентификатор уязвимости: CVE-2024-9463

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: Expedition: 1.0.91 - 1.2.95

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

46 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-11 / 2024-10-11

Ссылки на источник:

- <http://security.paloaltonetworks.com/PAN-SA-2024-0010>

Краткое описание: Выполнение произвольного кода в Siemens JT2Go

Идентификатор уязвимости: CVE-2024-41902

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: JT2Go: до 2406.0003

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

47 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-10 / 2024-10-10

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/html/ssa-626178.html>

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Nastran

Идентификатор уязвимости: CVE-2024-47046

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Simcenter Nastran: 2306 - 2406

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

48 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-10 / 2024-10-10

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/html/ssa-852501.html>

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Nastran

Идентификатор уязвимости: CVE-2024-41981

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Simcenter Nastran: 2306 - 2406

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

49 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-10 / 2024-10-10

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/html/ssa-852501.html>

Краткое описание: Получение конфиденциальной информации в wkhtmltopdf module for Drupal

Идентификатор уязвимости: None

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: wkhtmltopdf: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

50 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевое экранирования или другими административными мерами.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-10 / 2024-10-10

Ссылки на источник:

- <http://www.drupal.org/sa-contrib-2024-049>

Краткое описание: Выполнение произвольного кода в Junos Space

Идентификатор уязвимости: CVE-2024-39563

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: Juniper Junos Space: 24.1R1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

51

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-10 / 2024-10-10

Ссылки на источник:

- <http://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-Space-Remote-Command-Execution-RCE-vulnerability-in-web-application-CVE-2024-39563>

Краткое описание: Отказ в обслуживании в Junos OS Evolved

Идентификатор уязвимости: CVE-2024-47490

Идентификатор программной ошибки: CWE-923 Некорректная проверка конечной точки для канала связи

Уязвимый продукт: Junos OS Evolved: 21.4R1-EVO - 23.2R1-S2-EVO

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

52

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-10 / 2024-10-10

Ссылки на источник:

- <http://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Evolved-ACX-7000-Series-Receipt-of-specific-transit-MPLS-packets-causes-resources-to-be-exhausted-CVE-2024-47490>

Краткое описание: Выполнение произвольного кода в Mozilla Firefox , Firefox ESR и Thunderbird

Идентификатор уязвимости: CVE-2024-9680
BDU:2024-07929

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 131.0
Firefox ESR: 102.0 - 128.3.0
Firefox for Android: 100.1.0 - 131.0
Mozilla Thunderbird: 102.0 - 131.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

53 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- http://bugzilla.mozilla.org/show_bug.cgi?id=1923344
- <http://www.mozilla.org/security/advisories/mfsa2024-51/>
- <https://bdu.fstec.ru/vul/2024-07929>
- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-52/>

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45475

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

54 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45474

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

55 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45473

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

56 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45472

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

57 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45471

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

58 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45470

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

59 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45469

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

60 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45468

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

61 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45467

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

62 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Получение конфиденциальной информации в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45466

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

63 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Получение конфиденциальной информации в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45465

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

64 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Получение конфиденциальной информации в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45464

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

65 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Получение конфиденциальной информации в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-45463

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Tecnomatix Plant Simulation: до 2404.0005

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

66 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-583523.txt>

Краткое описание: Выполнение произвольного кода в Adobe Dimension

Идентификатор уязвимости: CVE-2024-45150

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Dimension: с версии 3.1 по 4.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

67 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/dimension/apsb24-74.html>

Краткое описание: Выполнение произвольного кода в Adobe Dimension

Идентификатор уязвимости: CVE-2024-45146

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Dimension: с версии 3.1 по 4.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

68

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/dimension/apsb24-74.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1332/>

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-45137

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Adobe InDesign: 18.0 - 19.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

69 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/indesign/apsb24-80.html>

Краткое описание: Выполнение произвольного кода в Adobe Framemaker

Идентификатор уязвимости: CVE-2024-47425

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: Adobe Framemaker: с версии 2017.0 по 2022.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

70 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/framemaker/apsb24-82.html>

Краткое описание: Выполнение произвольного кода в Adobe Framemaker

Идентификатор уязвимости: CVE-2024-47424

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Adobe Framemaker: с версии 2017.0 по 2022.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

71 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/framemaker/apsb24-82.html>

Краткое описание: Выполнение произвольного кода в Adobe Framemaker

Идентификатор уязвимости: CVE-2024-47423

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Adobe Framemaker: с версии 2017.0 по 2022.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

72 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/framemaker/apsb24-82.html>

Краткое описание: Выполнение произвольного кода в Adobe Framemaker

Идентификатор уязвимости: CVE-2024-47422

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Adobe Framemaker: с версии 2017.0 по 2022.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

73 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/framemaker/apsb24-82.html>

Краткое описание: Выполнение произвольного кода в Adobe Framemaker

Идентификатор уязвимости: CVE-2024-47421

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Framemaker: с версии 2017.0 по 2022.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

74 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/framemaker/apsb24-82.html>

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2024-47418

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Animate: с версии 20.0 по 24.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

75 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/animate/apsb24-76.html>

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2024-47417

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Animate: с версии 20.0 по 24.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

76 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/animate/apsb24-76.html>

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2024-47416

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Animate: с версии 20.0 по 24.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

77 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/animate/apsb24-76.html>

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2024-47415

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Animate: с версии 20.0 по 24.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

78 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/animate/apsb24-76.html>

Краткое описание: Выполнение произвольного кода в Adobe InCopy

Идентификатор уязвимости: CVE-2024-45136

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: InCopy: 18.0 - 19.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

79 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/incopy/apsb24-79.html>

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2024-47414

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Animate: с версии 20.0 по 24.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

80 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/animate/apsb24-76.html>

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2024-47413

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Animate: с версии 20.0 по 24.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

81 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/animate/apsb24-76.html>

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2024-47412

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Animate: с версии 20.0 по 24.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

82 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/animate/apsb24-76.html>

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2024-47411

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Animate: с версии 20.0 по 24.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

83 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/animate/apsb24-76.html>

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2024-47410

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Animate: с версии 20.0 по 24.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

84 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- <http://helpx.adobe.com/security/products/animate/apsb24-76.html>

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-9603

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 129.0.6668.90
Microsoft Edge: 79.0.309.71 - 129.0.2792.79

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

85

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_8.html
- <http://crbug.com/367818758>
- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-9603>

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-9602

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 129.0.6668.90
Microsoft Edge: 79.0.309.71 - 129.0.2792.79

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

86

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-10-09 / 2024-10-09

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_8.html
- <http://crbug.com/368241697>
- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-9602>

Краткое описание: Выполнение произвольного кода в Delta Electronics DIAEnergie

Идентификатор уязвимости: CVE-2024-42417

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: DIAEnergie: версии 1.10.01.008

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

87 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-07 / 2024-10-07

Ссылки на источник:

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-277-03>
- http://www.deltaww.com/en-US/Cybersecurity_Advisory

Краткое описание: Выполнение произвольного кода в Delta Electronics DIAEnergie

Идентификатор уязвимости: CVE-2024-43699

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: DIAEnergie: версии 1.10.01.008

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

88 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-07 / 2024-10-07

Ссылки на источник:

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-277-03>
- http://www.deltaww.com/en-US/Cybersecurity_Advisory

Краткое описание: Обход безопасности в Jenkins OpenId Connect Authentication plugin

Идентификатор уязвимости: CVE-2024-47807

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: OpenId Connect Authentication: версии 4.354.v321ce67a_1de8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

89 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-07 / 2024-10-07

Ссылки на источник:

- [http://www.jenkins.io/security/advisory/2024-10-02/#SECURITY-3441%20\(2\)](http://www.jenkins.io/security/advisory/2024-10-02/#SECURITY-3441%20(2))

Краткое описание: Обход безопасности в Jenkins OpenId Connect Authentication plugin

Идентификатор уязвимости: CVE-2024-47806

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: OpenId Connect Authentication: версии 4.354.v321ce67a_1de8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

90 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-07 / 2024-10-07

Ссылки на источник:

- [http://www.jenkins.io/security/advisory/2024-10-02/#SECURITY-3441%20\(1\)](http://www.jenkins.io/security/advisory/2024-10-02/#SECURITY-3441%20(1))

Краткое описание: Выполнение произвольного кода в GNOME libgsf

Идентификатор уязвимости: CVE-2024-36474

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: libgsf: с версии 1.14 по 1.14.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

91

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-07 / 2024-10-07

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2024-2068
- <http://gitlab.gnome.org/GNOME/libgsf/-/issues/34>

Краткое описание: Выполнение произвольного кода в GNOME libgsf

Идентификатор уязвимости: CVE-2024-42415

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: libgsf: с версии 1.14 по 1.14.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

92

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-07 / 2024-10-07

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2024-2069
- <http://gitlab.gnome.org/GNOME/libgsf/-/issues/34>

Краткое описание: Обход безопасности в Cisco IOS XE Software

Идентификатор уязвимости: CVE-2024-20510

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: Cisco IOS XE: с версии 17.6.4 по 17.9.4
Catalyst 9800-CL Wireless Controllers for Cloud: все версии
Catalyst 9800 Embedded Wireless Controller: все версии
Catalyst 9800 Series Wireless Controllers: все версии
Embedded Wireless Controllers on Catalyst Access Points: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса авторизации

93

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.3 AV:A/AC:L/PR:N/UI:N/S:C/H:I/N/A:N

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-26 / 2024-09-26

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9800-cwa-acl-nPSbHSnA>