НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2024-01-26.1 | 26 января 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-51698	Atril	Сетевой	ACE	2024-01-24	✓
2	Критическая	CVE-2024-20253	Cisco Unified Communications products	Сетевой	ACE	2024-01-24	✓
3	Критическая	CVE-2023-7227	SystemK NVR 504/508/516	Сетевой	ACE	2024-01-26	✗
4	Критическая	CVE-2023-46226	Apache IoTDB	Сетевой	ACE	2024-01-25	✓
5	Критическая	CVE-2024-23897	Jenkins and Jenkins LTS	Сетевой	ACE	2024-01-25	✓
6	Высокая	CVE-2024-0808	Microsoft Edge	Сетевой	ACE	2024-01-26	✓
7	Критическая	CVE-2024-21326	Microsoft Edge	Сетевой	ACE	2024-01-26	✓
8	Высокая	CVE-2024-21385	Microsoft Edge	Сетевой	OSI	2024-01-26	✓
9	Высокая	CVE-2024-0807	Microsoft Edge	Сетевой	ACE	2024-01-26	✓
10	Критическая	CVE-2024-0809	Microsoft Edge	Сетевой	OSI	2024-01-26	✓
11	Критическая	CVE-2024-0811	Microsoft Edge	Сетевой	OSI	2024-01-26	✓
12	Критическая	CVE-2024-0805	Microsoft Edge	Сетевой	OSI	2024-01-26	✓
13	Высокая	CVE-2024-0806	Microsoft Edge	Сетевой	OSI	2024-01-26	✓

14	Высокая	CVE-2024-0812	Microsoft Edge	Сетевой	OSI	2024-01-26	✓
15	Высокая	CVE-2023-49797	Intel In-Band Manageability Framework	Локальный	ACE	2024-01-24	✓
16	Высокая	CVE-2023-37920	Intel In-Band Manageability Framework	Сетевой	LoI	2024-01-24	✓
17	Высокая	CVE-2023-44487	Intel In-Band Manageability Framework	Сетевой	DoS	2024-01-24	✓
18	Высокая	CVE-2023-39325	Intel In-Band Manageability Framework	Сетевой	DoS	2024-01-24	✓
19	Критическая	CVE-2024-0204	GoAnywhere MFT	Сетевой	ACE	2024-01-24	✓

1

Краткое описание: Выполнение произвольного кода в Atril

Идентификатор уязвимости: CVE-2023-51698

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

Уязвимый продукт: atril: 1.10.0 - 1.27.0

Категория уязвимого продукта: Прикладное программное обеспечение

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: 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-24 / 2024-01-24

Ссылки на источник:

- http://github.com/mate-desktop/atril/security/advisories/GHSA-34rr-j8v9-v4p2
- http://github.com/mate-desktop/atril/commit/ce41df6467521ff9fd4f16514ae7d6ebb62eb1ed
- https://bdu.fstec.ru/vul/2024-00525

2

Краткое описание: Выполнение произвольного кода в Cisco Unified Communications products

Идентификатор уязвимости: CVE-2024-20253

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Cisco Packaged Contact Center Enterprise: 12.0.0 - 12.5.2
Cisco Unified Communications Manager: 11.5(1) - 14SU4
Cisco Unified Communications Manager IM & Presence Service: 11.0 - 14SU4
Cisco Unified Communications Manager Session Management Edition: 11.0 - 14SU3
Cisco Unified Contact Center Enterprise: 12.0 - 12.5.2
Cisco Unified Contact Center Express: 12.0 - 12.5.1 SU2
Cisco Unity Connection: 12.0 - 14SU3a
Cisco Virtualized Voice Browser: 12.5.0 - 12.5.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

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: 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: 2024-01-24 / 2024-01-24

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwd64245
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwd64276
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwd64292
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe18773
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe18830
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe18840

- https://bdu.fstec.ru/vul/2024-00719

3

Краткое описание: Выполнение произвольного кода в SystemK NVR 504/508/516

Идентификатор уязвимости: CVE-2023-7227

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

Уязвимый продукт: NVR 504: 2.3.5SK.30084998
NVR 508: 2.3.5SK.30084998
NVR 516: 2.3.5SK.30084998

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-025-02

4

Краткое описание: Выполнение произвольного кода в Apache IoTDB

Идентификатор уязвимости: CVE-2023-46226

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Apache IoTDB: 1.0.0 - 1.2.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-25 / 2024-01-25

Ссылки на источник:

- http://lists.apache.org/thread/293b4ob65ftnfwyf62fb9zh8gwdy38hg
- http://www.openwall.com/lists/oss-security/2024/01/15/1

Краткое описание: Выполнение произвольного кода в Jenkins and Jenkins LTS

Идентификатор уязвимости: CVE-2024-23897

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Jenkins и Jenkins LTS:
Jenkins: с версии 2.0 по 2.441
Jenkins LTS: с версии 2.7.1 по 2.426.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход ограничений безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-25 / 2024-01-25

Ссылки на источник:

- http://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3314
- http://www.openwall.com/lists/oss-security/2024/01/24/6

6

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-0808

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

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 120.0.2336.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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: 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: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0808

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-21326

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 120.0.2336.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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: 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21326

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-21385

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 120.0.2336.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21385

9

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-0807

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 120.0.2336.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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: 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: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0807

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-0809

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 120.0.2336.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0809

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-0811

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 120.0.2336.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0811

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-0805

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 120.0.2336.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0805

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-0806

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 120.0.2336.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: получение конфиденциальной информации

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: 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: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0806

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-0812

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 120.0.2336.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: получение конфиденциальной информации

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: 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: 2024-01-26 / 2024-01-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0812

Краткое описание: Выполнение произвольного кода в Intel In-Band Manageability Framework

Идентификатор уязвимости: CVE-2023-49797

Идентификатор программной ошибки: CWE-379 Создание временных файлов в каталоге, имеющем некорректные разрешения

Уязвимый продукт: Intel In-Band Manageability: с версии 2.6.2 по 4.1.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

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: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: 2024-01-24 / 2024-01-24

Ссылки на источник:

- http://github.com/intel/intel-inb-manageability/releases/tag/v4.2.0

16

Краткое описание: Потеря целостности в Intel In-Band Manageability Framework

Идентификатор уязвимости: CVE-2023-37920

Идентификатор программной ошибки: CWE-345 Некорректная проверка достоверности данных

Уязвимый продукт: Intel In-Band Manageability: с версии 2.6.2 по 4.1.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: потеря целостности

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:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-24 / 2024-01-24

Ссылки на источник:

- http://github.com/intel/intel-inb-manageability/releases/tag/v4.2.0
- https://bdu.fstec.ru/vul/2023-05463

17

Краткое описание: Отказ в обслуживании в Intel In-Band Manageability Framework

Идентификатор уязвимости: CVE-2023-44487

Идентификатор программной ошибки: CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

Уязвимый продукт: Intel In-Band Manageability: с версии 2.6.2 по 4.1.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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: 2024-01-24 / 2024-01-24

Ссылки на источник:

- http://github.com/intel/intel-inb-manageability/releases/tag/v4.2.0
- https://bdu.fstec.ru/vul/2023-06559

18

Краткое описание: Отказ в обслуживании в Intel In-Band Manageability Framework

Идентификатор уязвимости: CVE-2023-39325

Идентификатор программной ошибки: CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

Уязвимый продукт: Intel In-Band Manageability: с версии 2.6.2 по 4.1.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: отказ в обслуживании

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: 2024-01-24 / 2024-01-24

Ссылки на источник:

- http://github.com/intel/intel-inb-manageability/releases/tag/v4.2.0
- https://bdu.fstec.ru/vul/2023-07013

19

Краткое описание: Выполнение произвольного кода в GoAnywhere MFT

Идентификатор уязвимости: CVE-2024-0204

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: GoAnywhere MFT: с версии 6.0.0 по 7.4.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход процесса аутентификации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-24 / 2024-01-24

Ссылки на источник:

- http://www.fortra.com/security/advisory/fi-2024-001
- http://my.goanywhere.com/webclient/ViewSecurityAdvisories.xhtml
- http://www.horizon3.ai/cve-2024-0204-fortra-goanywhere-mft-authentication-bypass-deep-dive/
- https://bdu.fstec.ru/vul/2024-00665