НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-01-19.1 | 19 января 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-36478	Oracle Communications Cloud Native Core Network Exposure Function	Сетевой	DoS	2024-01-16	✓
2	Высокая	CVE-2023-5072	Oracle Communications Cloud Native Core Network Exposure Function	Сетевой	DoS	2024-01-16	✓
3	Высокая	CVE-2023-22102	Oracle	Сетевой	ACE	2024-01-16	✓
4	Высокая	CVE-2023-44487	Oracle	Сетевой	DoS	2024-01-16	✓
5	Высокая	CVE-2023-5072	Oracle Communications Cloud Native Core Unified Data Repository	Сетевой	DoS	2024-01-16	✓
6	Высокая	CVE-2023-1108	Oracle Communications Cloud Native Core Unified Data Repository	Сетевой	DoS	2024-01-16	✓
7	Высокая	CVE-2023-31582	Oracle	Сетевой	SB	2024-01-16	✓
8	Средняя	CVE-2023-34053	Oracle Communications Network Analytics Data Director	Сетевой	DoS	2024-01-16	✓
9	Средняя	CVE-2023-44483	Oracle	Сетевой	OSI	2024-01-16	✓
10	Средняя	CVE-2023-34055	Oracle Communications Cloud Native Core Console	Сетевой	DoS	2024-01-16	✓
11	Средняя	CVE-2023-2283	Oracle Communications Cloud Native Core Console	Сетевой	SB	2024-01-16	✓

12	Высокая	CVE-2022-3602	Oracle Essbase	Сетевой	ACE	2024-01-16	✓
13	Высокая	CVE-2023-42503	Oracle Essbase	Сетевой	DoS	2024-01-16	✓
14	Средняя	CVE-2024-20903	Oracle Database Server	Сетевой	OAF	2024-01-16	✓
15	Критическая	CVE-2023-38545	Oracle	Сетевой	ACE	2024-01-16	✓
16	Высокая	CVE-2024-0519	Google Chrome	Сетевой	ACE	2024-01-16	✓
17	Высокая	CVE-2024-0518	Google Chrome	Сетевой	ACE	2024-01-16	✓
18	Высокая	CVE-2024-0517	Google Chrome	Сетевой	ACE	2024-01-16	✓
19	Высокая	CVE-2024-20953	Oracle Agile PLM Framework	Сетевой	ACE	2024-01-17	✓
20	Критическая	CVE-2022-29155	Fujitsu M10-1	Сетевой	ACE	2024-01-17	✓
21	Критическая	CVE-2021-43527	Fujitsu M10-1	Сетевой	ACE	2024-01-17	✓
22	Высокая	CVE-2022-4450	Fujitsu M10-1	Сетевой	DoS	2024-01-17	✓
23	Высокая	CVE-2023-34624	Oracle Agile PLM Framework	Сетевой	DoS	2024-01-17	✓
24	Критическая	CVE-2023-38545	MySQL Cluster	Сетевой	ACE	2024-01-16	✓
25	Высокая	CVE-2023-39975	MySQL Cluster	Сетевой	DoS	2024-01-16	✓
26	Критическая	CVE-2022-42920	Oracle Retail Advanced Inventory Planning	Сетевой	ACE	2024-01-17	✓

27	Высокая	CVE-2023-5363	MySQL Workbench	Сетевой	OSI	2024-01-16	✓
28	Критическая	CVE-2023-50164	MySQL Enterprise Monitor	Сетевой	ACE	2024-01-16	✓
29	Высокая	CVE-2023-41105	MySQL Workbench	Сетевой	RLF	2024-01-16	✓
30	Высокая	CVE-2024-20932	Oracle GraalVM for JDK	Сетевой	RLF	2024-01-16	✓
31	Высокая	CVE-2023-46589	Oracle Communications Policy Management	Сетевой	RLF	2024-01-16	✓
32	Высокая	CVE-2023-5072	Oracle Communications Policy Management	Сетевой	DoS	2024-01-16	✓
33	Критическая	CVE-2023-46604	Oracle Communications Element Manager	Сетевой	ACE	2024-01-16	✓
34	Критическая	CVE-2023-34034	Oracle Communications Cloud Native Core Network Slice Selection Function	Сетевой	SB	2024-01-16	✓
35	Высокая	CVE-2023-22526	Atlassian Confluence Server and Data Center	Сетевой	ACE	2024-01-16	✓
36	Высокая	CVE-2024-21672	Atlassian Confluence Server and Data Center	Сетевой	ACE	2024-01-16	✓
37	Высокая	CVE-2023-6549	Citrix NetScaler ADC and NetScaler Gateway	Сетевой	DoS	2024-01-16	✓
38	Высокая	CVE-2024-21673	Atlassian Confluence Server and Data Center	Сетевой	ACE	2024-01-16	✓
39	Высокая	CVE-2024-21674	Atlassian Confluence Server and Data Center	Сетевой	OSI	2024-01-16	✓

40	Средняя	CVE-2023-6548	Citrix NetScaler ADC and NetScaler Gateway	Сетевой	ACE	2024-01-16	✓

1

Краткое описание: Отказ в обслуживании в Oracle Communications Cloud Native Core Network Exposure Function

Идентификатор уязвимости: CVE-2023-36478

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

Уязвимый продукт: Oracle Communications Cloud Native Core Network Exposure Function: 23.3.1

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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?952634

2

Краткое описание: Отказ в обслуживании в Oracle Communications Cloud Native Core Network Exposure Function

Идентификатор уязвимости: CVE-2023-5072

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Oracle Communications Cloud Native Core Network Exposure Function: 23.3.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?952634

Краткое описание: Выполнение произвольного кода в Oracle

Идентификатор уязвимости: CVE-2023-22102

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Communications Cloud Native Core Unified Data Repository: 23.3.1
Oracle Communications Cloud Native Core Network Exposure Function: 23.3.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?936690
- https://bdu.fstec.ru/vul/2023-07092

Краткое описание: Отказ в обслуживании в Oracle

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: Oracle Communications Cloud Native Core Unified Data Repository: 23.3.1
Oracle Communications Cloud Native Core Network Slice Selection Function: 23.2.0 - 23.3.1
Oracle Communications Network Analytics Data Director: 23.2.0.0.2 - 23.3.0.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: отказ в обслуживании

4

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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?936690
- https://bdu.fstec.ru/vul/2023-06559

5

Краткое описание: Отказ в обслуживании в Oracle Communications Cloud Native Core Unified Data Repository

Идентификатор уязвимости: CVE-2023-5072

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Oracle Communications Cloud Native Core Unified Data Repository: 23.3.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?936690

6

Краткое описание: Отказ в обслуживании в Oracle Communications Cloud Native Core Unified Data Repository

Идентификатор уязвимости: CVE-2023-1108

Идентификатор программной ошибки: CWE-835 Бесконечный цикл (зацикливание)

Уязвимый продукт: Oracle Communications Cloud Native Core Unified Data Repository: 23.3.1

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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?936690
- https://bdu.fstec.ru/vul/2023-01996

Краткое описание: Обход безопасности в Oracle

Идентификатор уязвимости: CVE-2023-31582

Идентификатор программной ошибки: CWE-331 Недостаточная энтропия

Уязвимый продукт: Oracle Communications Cloud Native Core Unified Data Repository: 23.3.1
Oracle Communications Cloud Native Core Network Exposure Function: 23.3.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Перебор JWT-токена

Последствия эксплуатации: обход безопасности

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: 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?936690

8

Краткое описание: Отказ в обслуживании в Oracle Communications Network Analytics Data Director

Идентификатор уязвимости: CVE-2023-34053

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Communications Network Analytics Data Director: 23.2.0.0.2 - 23.3.0.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?987622

Краткое описание: Получение конфиденциальной информации в Oracle

Идентификатор уязвимости: CVE-2023-44483

Идентификатор программной ошибки: CWE-532 Включение важной информации в файлы журналов

Уязвимый продукт: Oracle Communications Cloud Native Core Console: 23.3.1
Oracle Financial Services Analytical Applications Infrastructure: 8.0.7 - 8.1.2
Oracle Financial Services Behavior Detection Platform: 8.0.8.1 - 8.1.2.6
Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition: 8.0.8
Communications Service Catalog and Design: 7.4.2.8.0
PeopleSoft Enterprise PeopleTools: 8.59 - 8.61

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Создание подписи XML с включенным уровнем отладки.

9

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?936691
- https://bdu.fstec.ru/vul/2023-07354

Краткое описание: Отказ в обслуживании в Oracle Communications Cloud Native Core Console

Идентификатор уязвимости: CVE-2023-34055

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Communications Cloud Native Core Console: 23.3.1
Oracle Communications Network Analytics Data Director: 23.2.0.0.2 - 23.3.0.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: отказ в обслуживании

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?936691
- https://bdu.fstec.ru/vul/2023-09011

11

Краткое описание: Обход безопасности в Oracle Communications Cloud Native Core Console

Идентификатор уязвимости: CVE-2023-2283

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Oracle Communications Cloud Native Core Console: 23.3.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?936691
- https://bdu.fstec.ru/vul/2023-05381

12

Краткое описание: Выполнение произвольного кода в Oracle Essbase

Идентификатор уязвимости: CVE-2022-3602

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

Уязвимый продукт: Oracle Essbase: 21.5.3.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Использование специально созданного сертификата

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: 7.5 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?917625
- https://bdu.fstec.ru/vul/2022-06608

13

Краткое описание: Отказ в обслуживании в Oracle Essbase

Идентификатор уязвимости: CVE-2023-42503

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

Уязвимый продукт: Oracle Essbase: 21.5.3.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?917625
- https://bdu.fstec.ru/vul/2023-05808

14

Краткое описание: Перезапись произвольных файлов в Oracle Database Server

Идентификатор уязвимости: CVE-2024-20903

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Database Server: 19.3 - none

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: перезапись произвольных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?1408

Краткое описание: Выполнение произвольного кода в Oracle

Идентификатор уязвимости: CVE-2023-38545

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

Уязвимый продукт: Oracle Database Server: 19.3 - none
Oracle Essbase: 21.5.3.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

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: 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?1408
- https://bdu.fstec.ru/vul/2023-06576

16

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-0519

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 120.0.6099.217

Категория уязвимого продукта: Прикладное программное обеспечение

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/E:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html
- http://crbug.com/1517354

17

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-0518

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 120.0.6099.217

Категория уязвимого продукта: Прикладное программное обеспечение

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html
- http://crbug.com/1507412

18

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-0517

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 120.0.6099.217

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: 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html
- http://crbug.com/1515930

Краткое описание: Выполнение произвольного кода в Oracle Agile PLM Framework

Идентификатор уязвимости: CVE-2024-20953

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Agile PLM Framework: 9.3.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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:L/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: 2024-01-17 / 2024-01-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3261

Краткое описание: Выполнение произвольного кода в Fujitsu M10-1

Идентификатор уязвимости: CVE-2022-29155

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

Уязвимый продукт: Fujitsu M10-1: XCP2420 - XCP4030

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2024-01-17 / 2024-01-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3229
- https://bdu.fstec.ru/vul/2022-03203

21

Краткое описание: Выполнение произвольного кода в Fujitsu M10-1

Идентификатор уязвимости: CVE-2021-43527

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

Уязвимый продукт: Fujitsu M10-1: XCP2430 - XCP4040

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-01-17 / 2024-01-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3229
- https://bdu.fstec.ru/vul/2022-00002

22

Краткое описание: Отказ в обслуживании в Fujitsu M10-1

Идентификатор уязвимости: CVE-2022-4450

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Fujitsu M10-1: XCP2430 - XCP4040

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 2024-01-17 / 2024-01-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3229
- https://bdu.fstec.ru/vul/2023-02240

23

Краткое описание: Отказ в обслуживании в Oracle Agile PLM Framework

Идентификатор уязвимости: CVE-2023-34624

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Oracle Agile PLM Framework: 9.3.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

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: 2024-01-17 / 2024-01-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3261
- https://bdu.fstec.ru/vul/2023-04568

Краткое описание: Выполнение произвольного кода в MySQL Cluster

Идентификатор уязвимости: CVE-2023-38545

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

Уязвимый продукт: MySQL Cluster: 8.0.16 - 8.0.34

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?62368
- https://bdu.fstec.ru/vul/2023-06576

Краткое описание: Отказ в обслуживании в MySQL Cluster

Идентификатор уязвимости: CVE-2023-39975

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: MySQL Cluster: 8.0.16 - 8.0.34

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?62368

Краткое описание: Выполнение произвольного кода в Oracle Retail Advanced Inventory Planning

Идентификатор уязвимости: CVE-2022-42920

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Oracle Retail Advanced Inventory Planning: 15.0.3 - 16.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2024-01-17 / 2024-01-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?555817

27

Краткое описание: Получение конфиденциальной информации в MySQL Workbench

Идентификатор уязвимости: CVE-2023-5363

Идентификатор программной ошибки: CWE-310 Уязвимости, связанные с криптографией

Уязвимый продукт: MySQL Workbench: 8.0.11 - 8.0.34

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?62416
- https://bdu.fstec.ru/vul/2023-07691

28

Краткое описание: Выполнение произвольного кода в MySQL Enterprise Monitor

Идентификатор уязвимости: CVE-2023-50164

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: MySQL Enterprise Monitor: 8.0.0 - 8.0.36

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?61473
- https://bdu.fstec.ru/vul/2023-08547

29

Краткое описание: Чтение локальных файлов в MySQL Workbench

Идентификатор уязвимости: CVE-2023-41105

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: MySQL Workbench: 8.0.11 - 8.0.34

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: чтение локальных файлов

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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?62416

Краткое описание: Чтение локальных файлов в Oracle GraalVM for JDK

Идентификатор уязвимости: CVE-2024-20932

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle GraalVM for JDK: 17.0.9

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: чтение локальных файлов

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: 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?987627

31

Краткое описание: Чтение локальных файлов в Oracle Communications Policy Management

Идентификатор уязвимости: CVE-2023-46589

Идентификатор программной ошибки: CWE-444 Некорректная интерпретация HTTP-запросов (несанкционированные HTTP-запросы)

Уязвимый продукт: Oracle Communications Policy Management: 12.6.1.0.0 - 15.0.0.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: чтение локальных файлов

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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3291

Краткое описание: Отказ в обслуживании в Oracle Communications Policy Management

Идентификатор уязвимости: CVE-2023-5072

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Oracle Communications Policy Management: 12.6.1.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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: 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3291

33

Краткое описание: Выполнение произвольного кода в Oracle Communications Element Manager

Идентификатор уязвимости: CVE-2023-46604

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Oracle Communications Element Manager: 9.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?534788
- https://bdu.fstec.ru/vul/2023-07372

34

Краткое описание: Обход безопасности в Oracle Communications Cloud Native Core Network Slice Selection Function

Идентификатор уязвимости: CVE-2023-34034

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Oracle Communications Cloud Native Core Network Slice Selection Function: 23.2.0 - 23.3.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход процесса аутентификации

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: 9.1 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?936692
- https://bdu.fstec.ru/vul/2023-03799

Краткое описание: Выполнение произвольного кода в Atlassian Confluence Server and Data Center

Идентификатор уязвимости: CVE-2023-22526

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Atlassian Confluence Server: 7.13.0 - 8.7.1
Confluence Data Center: 7.13.0 - 8.7.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615
- http://jira.atlassian.com/browse/CONFSERVER-93516

Краткое описание: Выполнение произвольного кода в Atlassian Confluence Server and Data Center

Идентификатор уязвимости: CVE-2024-21672

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Confluence Data Center: 2.1 - 8.7.1
Atlassian Confluence Server: 2.1 - 8.7.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

36

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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://jira.atlassian.com/browse/CONFSERVER-94064

Краткое описание: Отказ в обслуживании в Citrix NetScaler ADC and NetScaler Gateway

Идентификатор уязвимости: CVE-2023-6549

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

Уязвимый продукт: Citrix Netscaler ADC: до 14.1-12.35
Citrix NetScaler Gateway: до 14.1-12.35

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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: 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: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://support.citrix.com/article/CTX584986
- https://bdu.fstec.ru/vul/2024-00383

Краткое описание: Выполнение произвольного кода в Atlassian Confluence Server and Data Center

Идентификатор уязвимости: CVE-2024-21673

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Atlassian Confluence Server: 7.13.0 - 8.7.1
Confluence Data Center: 7.13.0 - 8.7.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

38

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://jira.atlassian.com/browse/CONFSERVER-94065

Краткое описание: Получение конфиденциальной информации в Atlassian Confluence Server and Data Center

Идентификатор уязвимости: CVE-2024-21674

Идентификатор программной ошибки: CWE-200 Разглашение важной информации лицам без соответствующих прав

Уязвимый продукт: Atlassian Confluence Server: 7.13.0 - 8.7.1
Confluence Data Center: 7.13.0 - 8.7.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://jira.atlassian.com/browse/CONFSERVER-94066

Краткое описание: Выполнение произвольного кода в Citrix NetScaler ADC and NetScaler Gateway

Идентификатор уязвимости: CVE-2023-6548

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: Citrix Netscaler ADC: до 14.1-12.35
Citrix NetScaler Gateway: до 14.1-12.35

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://support.citrix.com/article/CTX584986