НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-04-19.1 | 19 апреля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-32460	FreeRDP	Сетевой	RLF	2024-04-19	✓
2	Высокая	CVE-2024-32459	FreeRDP	Сетевой	RLF	2024-04-19	✓
3	Высокая	CVE-2024-32458	FreeRDP	Сетевой	RLF	2024-04-19	✓
4	Критическая	CVE-2024-32040	FreeRDP	Сетевой	ACE	2024-04-19	✓
5	Критическая	CVE-2024-32039	FreeRDP	Сетевой	ACE	2024-04-19	✓
6	Высокая	CVE-2024-32041	FreeRDP	Сетевой	RLF	2024-04-19	✓
7	Критическая	CVE-2024-2961	GNU C Library	Сетевой	ACE	2024-04-18	✓
8	Критическая	CVE-2024-28890	Forminator plugin for WordPress	Сетевой	ACE	2024-04-18	✓
9	Высокая	CVE-2024-20295	Cisco Integrated Management Controller	Локальный	ACE	2024-04-18	✓
10	Высокая	CVE-2024-20356	Cisco Integrated Management Controller	Сетевой	ACE	2024-04-18	✓
11	Высокая	CVE-2024-3493	Rockwell Automation ControlLogix and GuardLogix	Сетевой	DoS	2024-04-17	✓
12	Высокая	CVE-2024-3914	Google Chrome	Сетевой	ACE	2024-04-17	✓
13	Высокая	CVE-2024-3838	Google Chrome	Сетевой	OSI	2024-04-17	✓

14	Высокая	CVE-2024-3834	Google Chrome	Сетевой	ACE	2024-04-17	✓
15	Высокая	CVE-2024-3833	Google Chrome	Сетевой	ACE	2024-04-17	✓
16	Высокая	CVE-2024-3832	Google Chrome	Сетевой	ACE	2024-04-17	✓
17	Высокая	CVE-2024-0743	Oracle Linux	Сетевой	ACE	2024-04-17	✓
18	Высокая	CVE-2024-2607	Oracle Linux	Сетевой	ACE	2024-04-17	✓
19	Высокая	CVE-2024-2608	Oracle Linux	Сетевой	ACE	2024-04-17	✓
20	Высокая	CVE-2024-1394	Oracle Linux	Сетевой	DoS	2024-04-17	✓
21	Высокая	CVE-2024-27316	Oracle Linux	Сетевой	DoS	2024-04-17	✓
22	Высокая	CVE-2024-22019	Oracle Linux	Сетевой	DoS	2024-04-17	✓
23	Высокая	CVE-2024-2614	Oracle Linux	Сетевой	ACE	2024-04-17	✓
24	Высокая	CVE-2024-25111	Oracle Linux	Сетевой	DoS	2024-04-17	✓
25	Высокая	CVE-2024-21892	Oracle Linux	Локальный	PE	2024-04-17	✓
26	Высокая	CVE-2024-1488	Oracle Linux	Локальный	SB	2024-04-17	✓
27	Высокая	CVE-2024-21896	Oracle Linux	Локальный	RLF	2024-04-17	✓
28	Высокая	CVE-2024-31083	Oracle Linux	Локальный	ACE	2024-04-17	✓

29	Высокая	CVE-2024-1086	Oracle Linux	Локальный	ACE	2024-04-17	✓
30	Высокая	CVE-2024-21891	Oracle Linux	Локальный	RLF	2024-04-17	✓
31	Высокая	CVE-2024-29944	Oracle Linux	Сетевой	ACE	2024-04-17	✓
32	Критическая	CVE-2024-2201	Oracle Linux	Смежная сеть	PE	2024-04-17	✓
33	Критическая	CVE-2024-1597	Oracle Linux	Сетевой	ACE	2024-04-17	✓
34	Высокая	CVE-2024-2612	Oracle Linux	Сетевой	ACE	2024-04-17	✓
35	Высокая	CVE-2024-21092	Oracle Agile Product Lifecycle Management for Process	Сетевой	WLF	2024-04-17	✓
36	Высокая	CVE-2024-21626	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	Локальный	ACE	2024-04-16	✓
37	Высокая	CVE-2024-25062	Oracle Communications Cloud Native Core Network Function Cloud Native Environment	Сетевой	ACE	2024-04-16	✓
38	Высокая	CVE-2024-22257	Oracle Communications Cloud Native Core Policy	Сетевой	SB	2024-04-16	✓
39	Высокая	CVE-2024-26130	Oracle Communications Cloud Native Core Policy	Сетевой	DoS	2024-04-16	✓
40	Высокая	CVE-2024-22201	Oracle Communications Cloud Native Core Policy	Сетевой	DoS	2024-04-16	✓

41	Высокая	CVE-2024-22233	Oracle Communications Cloud Native Core Security Edge Protection Proxy	Сетевой	DoS	2024-04-16	✓
42	Высокая	CVE-2024-21095	Primavera P6 Enterprise Project Portfolio Management	Сетевой	WLF	2024-04-16	✓
43	Критическая	CVE-2023-41993	Oracle GraalVM Enterprise Edition и Oracle Java SE	Сетевой	ACE	2024-04-17	✓
44	Критическая	CVE-2024-20997	Oracle Hospitality Simphony	Сетевой	ACE	2024-04-17	✓
45	Критическая	CVE-2024-21010	Oracle Hospitality Simphony	Сетевой	ACE	2024-04-17	✓
46	Критическая	CVE-2024-21014	Oracle Hospitality Simphony	Сетевой	ACE	2024-04-17	✓
47	Критическая	CVE-2022-46337	Oracle Enterprise Data Quality	Сетевой	SB	2024-04-17	✓
48	Критическая	CVE-2024-1597	Oracle Enterprise Data Quality	Сетевой	ACE	2024-04-17	✓
49	Высокая	CVE-2024-26308	Oracle Enterprise Data Quality	Сетевой	DoS	2024-04-17	✓
50	Высокая	CVE-2024-3865	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2024-04-17	✓
51	Высокая	CVE-2024-3856	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2024-04-17	✓
52	Высокая	CVE-2024-3855	Mozilla Firefox and Firefox ESR	Сетевой	OSI	2024-04-17	✓
53	Высокая	CVE-2024-3853	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2024-04-17	✓
54	Высокая	CVE-2024-3854	Mozilla Firefox and Firefox ESR	Сетевой	OSI	2024-04-17	✓

55	Высокая	CVE-2024-3857	Mozilla Firefox and Firefox ESR	Сетевой	OSI	2024-04-17	✓
56	Высокая	CVE-2024-3852	Mozilla Firefox and Firefox ESR	Сетевой	OSI	2024-04-17	✓
57	Высокая	CVE-2024-3864	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2024-04-17	✓
58	Высокая	CVE-2024-21006	Oracle WebLogic Server	Сетевой	OSI	2024-04-17	✓
59	Высокая	CVE-2024-21007	Oracle WebLogic Server	Сетевой	OSI	2024-04-17	✓
60	Высокая	CVE-2024-26308	Oracle WebLogic Server	Сетевой	DoS	2024-04-17	✓
61	Критическая	CVE-2024-21082	Oracle BI Publisher	Сетевой	ACE	2024-04-17	✓
62	Высокая	CVE-2024-26308	Oracle Communications Unified Inventory Management	Сетевой	DoS	2024-04-17	✓
63	Критическая	CVE-2023-47100	Oracle Communications Cloud Native Core Network Repository Function	Сетевой	ACE	2024-04-17	✓
64	Высокая	CVE-2023-41056	Oracle Communications Cloud Native Core Network Repository Function	Сетевой	ACE	2024-04-17	✓
65	Высокая	CVE-2023-44487	Oracle Communications Cloud Native Core Network Repository Function	Сетевой	DoS	2024-04-17	✓
66	Высокая	CVE-2024-1635	Oracle Communications Cloud Native Core Network Repository Function	Сетевой	DoS	2024-04-17	✓
67	Высокая	CVE-2024-21067	Enterprise Manager Base Platform	Локальный	ACE	2024-04-17	✓
68	Высокая	CVE-2024-0727	the Siemens SIMATIC S7-1500 TM MFP	Сетевой	DoS	2024-04-15	✗

69	Высокая	CVE-2023-45898	the Siemens SIMATIC S7-1500 TM MFP	Локальный	PE	2024-04-15	✗
70	Высокая	CVE-2023-6932	the Siemens SIMATIC S7-1500 TM MFP	Локальный	ACE	2024-04-15	✗
71	Высокая	CVE-2023-6931	the Siemens SIMATIC S7-1500 TM MFP	Локальный	ACE	2024-04-15	✗
72	Высокая	CVE-2023-6817	the Siemens SIMATIC S7-1500 TM MFP	Локальный	PE	2024-04-15	✗
73	Высокая	CVE-2024-31978	Siemens SINEC NMS	Сетевой	OSI	2024-04-15	✓
74	Критическая	CVE-2024-3400	Palo Alto PAN-OS	Сетевой	ACE	2024-04-12	✓
75	Критическая	CVE-2024-3383	Palo Alto PAN-OS	Сетевой	OSI	2024-04-12	✓

1

Краткое описание: Чтение локальных файлов в FreeRDP

Идентификатор уязвимости: CVE-2024-32460

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FreeRDP: 2.11.0 - 3.4.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

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:H/I:N/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-19 / 2024-04-19

Ссылки на источник:

- http://github.com/FreeRDP/FreeRDP/releases/tag/2.11.6
- http://github.com/FreeRDP/FreeRDP/releases/tag/3.5.0

2

Краткое описание: Чтение локальных файлов в FreeRDP

Идентификатор уязвимости: CVE-2024-32459

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FreeRDP: 2.11.0 - 3.4.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

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:H/I:N/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-19 / 2024-04-19

Ссылки на источник:

- http://github.com/FreeRDP/FreeRDP/releases/tag/2.11.6
- http://github.com/FreeRDP/FreeRDP/releases/tag/3.5.0

3

Краткое описание: Чтение локальных файлов в FreeRDP

Идентификатор уязвимости: CVE-2024-32458

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FreeRDP: 2.11.0 - 3.4.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

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:H/I:N/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-19 / 2024-04-19

Ссылки на источник:

- http://github.com/FreeRDP/FreeRDP/releases/tag/2.11.6
- http://github.com/FreeRDP/FreeRDP/releases/tag/3.5.0

4

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2024-32040

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

Уязвимый продукт: FreeRDP: 2.11.0 - 3.4.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданных запросов.

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: 2024-04-19 / 2024-04-19

Ссылки на источник:

- http://github.com/FreeRDP/FreeRDP/releases/tag/2.11.6
- http://github.com/FreeRDP/FreeRDP/releases/tag/3.5.0

5

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2024-32039

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

Уязвимый продукт: FreeRDP: 2.11.0 - 3.4.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2024-04-19 / 2024-04-19

Ссылки на источник:

- http://github.com/FreeRDP/FreeRDP/releases/tag/2.11.6
- http://github.com/FreeRDP/FreeRDP/releases/tag/3.5.0

6

Краткое описание: Чтение локальных файлов в FreeRDP

Идентификатор уязвимости: CVE-2024-32041

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FreeRDP: 2.11.0 - 3.4.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

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:H/I:N/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-19 / 2024-04-19

Ссылки на источник:

- http://github.com/FreeRDP/FreeRDP/releases/tag/2.11.6
- http://github.com/FreeRDP/FreeRDP/releases/tag/3.5.0

7

Краткое описание: Выполнение произвольного кода в GNU C Library

Идентификатор уязвимости: CVE-2024-2961

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

Уязвимый продукт: Glibc: 0.1 - 5.3.12

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2024-04-18 / 2024-04-18

Ссылки на источник:

- http://sourceware.org/git/?p=glibc.git;a=blob;f=advisories/GLIBC-SA-2024-0004

8

Краткое описание: Выполнение произвольного кода в Forminator plugin for WordPress

Идентификатор уязвимости: CVE-2024-28890

Идентификатор программной ошибки: CWE-434 Отсутствие ограничений на загрузку файлов небезопасного типа

Уязвимый продукт: Forminator Contact Form, Poll & Quiz Builder: 1.5.1 - 1.28.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-18 / 2024-04-18

Ссылки на источник:

- http://jvn.jp/en/jp/JVN50132400/index.html

Краткое описание: Выполнение произвольного кода в Cisco Integrated Management Controller

Идентификатор уязвимости: CVE-2024-20295

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

Уязвимый продукт: Cisco Integrated Management Controller: 3.2.6 - 4.12
Enterprise NFV Infrastructure Software: 3.12 - 3.13
Cisco 5000 Series Enterprise Network Compute System: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

9 **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: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: 2024-04-18 / 2024-04-18

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-mUx4c5AJ

Краткое описание: Выполнение произвольного кода в Cisco Integrated Management Controller

Идентификатор уязвимости: CVE-2024-20356

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

Уязвимый продукт: Cisco Integrated Management Controller: 3.1 - 4.12
Enterprise NFV Infrastructure Software: 3.12 - 3.13
Cisco 5000 Series Enterprise Network Compute System: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

10 **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: 8.7 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-18 / 2024-04-18

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb

11

Краткое описание: Отказ в обслуживании в Rockwell Automation ControlLogix and GuardLogix

Идентификатор уязвимости: CVE-2024-3493

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ControlLogix 5580: 35.011
GuardLogix 5580: 35.011
CompactLogix 5380: 35.011
1756-EN4TR: 5.001

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/support/advisory.SD1666.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-107-03

12

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-3914

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.123

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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html
- http://issues.chromium.org/issues/330759272

13

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-3838

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.123

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html
- http://crbug.com/328278717

14

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-3834

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.123

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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html
- http://crbug.com/326607008

15

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-3833

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.123

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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html
- http://crbug.com/331383939

16

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-3832

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.123

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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html
- http://crbug.com/331358160

17

Краткое описание: Выполнение произвольного кода в Oracle Linux

Идентификатор уязвимости: CVE-2024-0743

Идентификатор программной ошибки: CWE-252 Отсутствует проверка возвращаемых значений

Уязвимый продукт: Oracle Linux: все версии

Категория уязвимого продукта: Unix-подобные операционные системы 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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-00804

18

Краткое описание: Выполнение произвольного кода в Oracle Linux

Идентификатор уязвимости: CVE-2024-2607

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

Уязвимый продукт: Oracle Linux: все версии

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

Способ эксплуатации: Не определено

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:H/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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-02315

19

Краткое описание: Выполнение произвольного кода в Oracle Linux

Идентификатор уязвимости: CVE-2024-2608

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

Уязвимый продукт: Oracle Linux: все версии

Категория уязвимого продукта: Unix-подобные операционные системы 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-02316

20

Краткое описание: Отказ в обслуживании в Oracle Linux

Идентификатор уязвимости: CVE-2024-1394

Идентификатор программной ошибки: CWE-401 Некорректное освобождение памяти до удаления последней ссылки (утечка памяти)

Уязвимый продукт: Oracle Linux: все версии

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-02371

21

Краткое описание: Отказ в обслуживании в Oracle Linux

Идентификатор уязвимости: CVE-2024-27316

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

Уязвимый продукт: Oracle Linux: все версии

Категория уязвимого продукта: Unix-подобные операционные системы и их 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-02653

22

Краткое описание: Отказ в обслуживании в Oracle Linux

Идентификатор уязвимости: CVE-2024-22019

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Linux: все версии

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-02798

23

Краткое описание: Выполнение произвольного кода в Oracle Linux

Идентификатор уязвимости: CVE-2024-2614

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

Уязвимый продукт: Oracle Linux: все версии

Категория уязвимого продукта: Unix-подобные операционные системы 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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-02327

24

Краткое описание: Отказ в обслуживании в Oracle Linux

Идентификатор уязвимости: CVE-2024-25111

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: Oracle Linux: все версии

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-02061

Краткое описание: Повышение привилегий в Oracle Linux

Идентификатор уязвимости: CVE-2024-21892

Идентификатор программной ошибки: CWE-755 Некорректная обработка исключений

Уязвимый продукт: Oracle Linux: все версии

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Повышение привилегий

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-01672

Краткое описание: Обход безопасности в Oracle Linux

Идентификатор уязвимости: CVE-2024-1488

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Oracle Linux: все версии

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

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Обход безопасности

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html

27

Краткое описание: Чтение локальных файлов в Oracle Linux

Идентификатор уязвимости: CVE-2024-21896

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

Уязвимый продукт: Oracle Linux: все версии

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-02879

Краткое описание: Выполнение произвольного кода в Oracle Linux

Идентификатор уязвимости: CVE-2024-31083

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Oracle Linux: все версии

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

Способ эксплуатации: Не определено

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html

29

Краткое описание: Выполнение произвольного кода в Oracle Linux

Идентификатор уязвимости: CVE-2024-1086

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Oracle Linux: все версии

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

Способ эксплуатации: Не определено

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-01187

Краткое описание: Чтение локальных файлов в Oracle Linux

Идентификатор уязвимости: CVE-2024-21891

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

Уязвимый продукт: Oracle Linux: все версии

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

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html

31

Краткое описание: Выполнение произвольного кода в Oracle Linux

Идентификатор уязвимости: CVE-2024-29944

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

Уязвимый продукт: Oracle Linux: все версии

Категория уязвимого продукта: Unix-подобные операционные системы 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-02304

Краткое описание: Повышение привилегий в Oracle Linux

Идентификатор уязвимости: CVE-2024-2201

Идентификатор программной ошибки: CWE-1037 Удаление или изменение обеспечивающего безопасность кода при оптимизации процессором

Уязвимый продукт: Oracle Linux: все версии

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html

Краткое описание: Выполнение произвольного кода в Oracle Linux

Идентификатор уязвимости: CVE-2024-1597

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

Уязвимый продукт: Oracle Linux: все версии

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

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-01541

34

Краткое описание: Выполнение произвольного кода в Oracle Linux

Идентификатор уязвимости: CVE-2024-2612

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Oracle Linux: все версии

Категория уязвимого продукта: Unix-подобные операционные системы 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/linuxbulletinapr2024.html
- https://bdu.fstec.ru/vul/2024-02333

Краткое описание: Запись локальных файлов в Oracle Agile Product Lifecycle Management for Process

Идентификатор уязвимости: CVE-2024-21092

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Agile Product Lifecycle Management for Process: 6.2.4.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Запись локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?3358

Краткое описание: Выполнение произвольного кода в Oracle Communications Cloud Native Core Network Function Cloud Native Environment

Идентификатор уязвимости: CVE-2024-21626

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Oracle Communications Cloud Native Core Network Function Cloud Native Environment: 23.4.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-16 / 2024-04-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?936688
- https://bdu.fstec.ru/vul/2024-00973

Краткое описание: Выполнение произвольного кода в Oracle Communications Cloud Native Core Network Function Cloud Native Environment

Идентификатор уязвимости: CVE-2024-25062

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Oracle Communications Cloud Native Core Network Function Cloud Native Environment: 23.4.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка 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: 7.5 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: 2024-04-16 / 2024-04-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?936688
- https://bdu.fstec.ru/vul/2024-01415

38

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

Идентификатор уязвимости: CVE-2024-22257

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Oracle Communications Cloud Native Core Policy: 23.4.0 - 23.4.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход ограничений безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-16 / 2024-04-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?936689
- https://bdu.fstec.ru/vul/2024-02143

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

Идентификатор уязвимости: CVE-2024-26130

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Oracle Communications Cloud Native Core Policy: 23.4.0 - 23.4.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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: 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: 2024-04-16 / 2024-04-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?936689

40

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

Идентификатор уязвимости: CVE-2024-22201

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

Уязвимый продукт: Oracle Communications Cloud Native Core Policy: 23.4.0 - 23.4.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 2024-04-16 / 2024-04-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?936689

41

Краткое описание: Отказ в обслуживании в Oracle Communications Cloud Native Core Security Edge Protection Proxy

Идентификатор уязвимости: CVE-2024-22233

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Communications Cloud Native Core Security Edge Protection Proxy: 23.4.0

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: 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: 2024-04-16 / 2024-04-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?936686
- https://bdu.fstec.ru/vul/2024-00777

Краткое описание: Запись локальных файлов в Primavera P6 Enterprise Project Portfolio Management

Идентификатор уязвимости: CVE-2024-21095

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Primavera P6 Enterprise Project Portfolio Management: 19.12.0 - 23.12.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Запись локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-16 / 2024-04-16

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?3194

Краткое описание: Выполнение произвольного кода в Oracle GraalVM Enterprise Edition и Oracle Java SE

Идентификатор уязвимости: CVE-2023-41993

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

Уязвимый продукт: Oracle GraalVM Enterprise Edition: 20.3.13 - 21.3.9
Oracle Java SE: 8u401

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?505601
- http://www.oracle.com/security-alerts/cpuapr2024.html?3082
- https://bdu.fstec.ru/vul/2023-06113

Краткое описание: Выполнение произвольного кода в Oracle Hospitality Simphony

Идентификатор уязвимости: CVE-2024-20997

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Hospitality Simphony: 19.1.0 - 19.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

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: 9.9 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?917576

Краткое описание: Выполнение произвольного кода в Oracle Hospitality Simphony

Идентификатор уязвимости: CVE-2024-21010

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Hospitality Simphony: 19.1.0 - 19.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

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:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?917576

Краткое описание: Выполнение произвольного кода в Oracle Hospitality Simphony

Идентификатор уязвимости: CVE-2024-21014

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Hospitality Simphony: 19.1.0 - 19.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?917576

Краткое описание: Обход безопасности в Oracle Enterprise Data Quality

Идентификатор уязвимости: CVE-2022-46337

Идентификатор программной ошибки: CWE-90 Некорректная нейтрализация специальных элементов, используемых в LDAP-запросах (внедрение LDAP)

Уязвимый продукт: Oracle Enterprise Data Quality: 12.2.1.4.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Обход безопасности

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?924165
- https://bdu.fstec.ru/vul/2024-00180

Краткое описание: Выполнение произвольного кода в Oracle Enterprise Data Quality

Идентификатор уязвимости: CVE-2024-1597

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

Уязвимый продукт: Oracle Enterprise Data Quality: 12.2.1.4.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?924165
- https://bdu.fstec.ru/vul/2024-01541

Краткое описание: Отказ в обслуживании в Oracle Enterprise Data Quality

Идентификатор уязвимости: CVE-2024-26308

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

Уязвимый продукт: Oracle Enterprise Data Quality: 12.2.1.4.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

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: 7.5 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?924165
- https://bdu.fstec.ru/vul/2024-02799

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-3865

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

Уязвимый продукт: Mozilla Firefox: 116.0 - 124.0.2
Firefox for Android: 116.0 - 124.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

50

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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-18/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-3856

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 116.0 - 124.0.2
Firefox for Android: 116.0 - 124.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-18/

52

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-3855

Идентификатор программной ошибки: CWE-1037 Удаление или изменение обеспечивающего безопасность кода при оптимизации процессором

Уязвимый продукт: Mozilla Firefox: 116.0 - 124.0.2
Firefox for Android: 116.0 - 124.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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:H/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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-18/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-3853

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 116.0 - 124.0.2
Firefox for Android: 116.0 - 124.2.0

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:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-18/

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-3854

Идентификатор программной ошибки: CWE-1037 Удаление или изменение обеспечивающего безопасность кода при оптимизации процессором

Уязвимый продукт: Mozilla Firefox: 100.0 - 124.0.2
Firefox ESR: 102.0 - 115.9.1
Firefox for Android: 100.1.0 - 124.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-18/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-19/

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-3857

Идентификатор программной ошибки: CWE-1037 Удаление или изменение обеспечивающего безопасность кода при оптимизации процессором

Уязвимый продукт: Mozilla Firefox: 100.0 - 124.0.2
Firefox ESR: 102.0 - 115.9.1
Firefox for Android: 100.1.0 - 124.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-18/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-19/

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-3852

Идентификатор программной ошибки: CWE-1037 Удаление или изменение обеспечивающего безопасность кода при оптимизации процессором

Уязвимый продукт: Mozilla Firefox: 100.0 - 124.0.2
Firefox ESR: 102.0 - 115.9.1
Firefox for Android: 100.1.0 - 124.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-18/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-19/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-3864

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 124.0.2
Firefox ESR: 102.0 - 115.9.1
Firefox for Android: 100.1.0 - 124.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-18/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-19/

58

Краткое описание: Получение конфиденциальной информации в Oracle WebLogic Server

Идентификатор уязвимости: CVE-2024-21006

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle WebLogic Server: 12.2.1.4.0 - 14.1.1.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?3219

Краткое описание: Получение конфиденциальной информации в Oracle WebLogic Server

Идентификатор уязвимости: CVE-2024-21007

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle WebLogic Server: 12.2.1.4.0 - 14.1.1.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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: 7.5 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?3219

60

Краткое описание: Отказ в обслуживании в Oracle WebLogic Server

Идентификатор уязвимости: CVE-2024-26308

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

Уязвимый продукт: Oracle WebLogic Server: 14.1.1.0.0

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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?3219
- https://bdu.fstec.ru/vul/2024-02799

Краткое описание: Выполнение произвольного кода в Oracle BI Publisher

Идентификатор уязвимости: CVE-2024-21082

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle BI Publisher: 7.0.0.0.0 - 12.2.1.4.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?3240

62

Краткое описание: Отказ в обслуживании в Oracle Communications Unified Inventory Management

Идентификатор уязвимости: CVE-2024-26308

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

Уязвимый продукт: Oracle Communications Unified Inventory Management: 7.4.0 - 7.5.0

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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?504206
- https://bdu.fstec.ru/vul/2024-02799

63

Краткое описание: Выполнение произвольного кода в Oracle Communications Cloud Native Core Network Repository Function

Идентификатор уязвимости: CVE-2023-47100

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Communications Cloud Native Core Network Repository Function: 23.4.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?947626
- https://bdu.fstec.ru/vul/2023-08382

64

Краткое описание: Выполнение произвольного кода в Oracle Communications Cloud Native Core Network Repository Function

Идентификатор уязвимости: CVE-2023-41056

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

Уязвимый продукт: Oracle Communications Cloud Native Core Network Repository Function: 23.4.1

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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?947626
- https://bdu.fstec.ru/vul/2024-00349

65

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

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: Oracle Communications Cloud Native Core Network Repository Function: 23.4.1

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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?947626
- https://bdu.fstec.ru/vul/2023-06559

66

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

Идентификатор уязвимости: CVE-2024-1635

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

Уязвимый продукт: Oracle Communications Cloud Native Core Network Repository Function: 23.4.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?947626

67

Краткое описание: Выполнение произвольного кода в Enterprise Manager Base Platform

Идентификатор уязвимости: CVE-2024-21067

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Enterprise Manager Base Platform: 13.5.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных 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: 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: 2024-04-17 / 2024-04-17

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpuapr2024.html?3207

Краткое описание: Отказ в обслуживании в the Siemens SIMATIC S7-1500 TM MFP

Идентификатор уязвимости: CVE-2024-0727

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: SIMATIC S7-1500 TM MFP: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Использование специально созданного вредоносного сертификата.

Последствия эксплуатации: Отказ в обслуживании

68 **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/E:U/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-15 / 2024-04-15

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-265688.txt
- https://bdu.fstec.ru/vul/2024-01337

Краткое описание: Повышение привилегий в the Siemens SIMATIC S7-1500 TM MFP

Идентификатор уязвимости: CVE-2023-45898

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SIMATIC S7-1500 TM MFP: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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: 2024-04-15 / 2024-04-15

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-265688.txt
- https://bdu.fstec.ru/vul/2023-07000

Краткое описание: Выполнение произвольного кода в the Siemens SIMATIC S7-1500 TM MFP

Идентификатор уязвимости: CVE-2023-6932

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SIMATIC S7-1500 TM MFP: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2024-04-15 / 2024-04-15

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-265688.txt
- https://bdu.fstec.ru/vul/2023-09022

Краткое описание: Выполнение произвольного кода в the Siemens SIMATIC S7-1500 TM MFP

Идентификатор уязвимости: CVE-2023-6931

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: SIMATIC S7-1500 TM MFP: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2024-04-15 / 2024-04-15

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-265688.txt
- https://bdu.fstec.ru/vul/2023-09023

Краткое описание: Повышение привилегий в the Siemens SIMATIC S7-1500 TM MFP

Идентификатор уязвимости: CVE-2023-6817

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SIMATIC S7-1500 TM MFP: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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: 2024-04-15 / 2024-04-15

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-265688.txt
- https://bdu.fstec.ru/vul/2023-08958

Краткое описание: Получение конфиденциальной информации в Siemens SINEC NMS

Идентификатор уязвимости: CVE-2024-31978

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

Уязвимый продукт: SINEC NMS: до 2.0 SP2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-15 / 2024-04-15

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-128433.txt

Краткое описание: Выполнение произвольного кода в Palo Alto PAN-OS

Идентификатор уязвимости: CVE-2024-3400

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

Уязвимый продукт: Palo Alto PAN-OS: 10.2 - 11.1.2-h2

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

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-12 / 2024-04-12

Ссылки на источник:

- http://security.paloaltonetworks.com/CVE-2024-3400

Краткое описание: Получение конфиденциальной информации в Palo Alto PAN-OS

Идентификатор уязвимости: CVE-2024-3383

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: Palo Alto PAN-OS: 10.1 - 11.0.2-h3

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-12 / 2024-04-12

Ссылки на источник:

- http://security.paloaltonetworks.com/CVE-2024-3383