НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-11-01.1 | 1 ноября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-29155	INEA ME RTU	Сетевой	SB	2023-11-01	✓
2	Критическая	CVE-2023-35762	INEA ME RTU	Сетевой	ACE	2023-11-01	✓
3	Высокая	CVE-2023-4249	Zavio IP Cameras	Сетевой	ACE	2023-11-01	✗
4	Высокая	CVE-2023-39435	Zavio IP Cameras	Сетевой	ACE	2023-11-01	✗
5	Критическая	CVE-2023-43755	Zavio IP Cameras	Сетевой	ACE	2023-11-01	✗
6	Критическая	CVE-2023-45225	Zavio IP Cameras	Сетевой	ACE	2023-11-01	✗
7	Критическая	CVE-2023-3959	Zavio IP Cameras	Сетевой	ACE	2023-11-01	✗
8	Критическая	CVE-2023-22518	Confluence Server and Data Center	Сетевой	OAF	2023-10-31	✓
9	Высокая	CVE-2023-22514	Atlassian Sourcetree for Windows	Локальный	ACE	2023-10-31	✓
10	Критическая	CVE-2023-46509	Contec SolarView Compact	Сетевой	ACE	2023-10-30	✗
11	Критическая	CVE-2023-42406	D-Link DAR-7000	Сетевой	ACE	2023-10-30	✗
12	Высокая	CVE-2023-5426	Post Meta Data Manager plugin for WordPress	Сетевой	OAF	2023-10-30	✓
13	Высокая	CVE-2023-5425	Post Meta Data Manager plugin for WordPress	Сетевой	PE	2023-10-30	✓

14	Высокая	CVE-2022-4886	Ingress-NGINX Controller for Kubernetes	Сетевой	OSI	2023-10-30	✓
15	Высокая	CVE-2023-5044	Ingress-NGINX Controller for Kubernetes	Сетевой	ACE	2023-10-30	✓
16	Высокая	CVE-2023-5043	Ingress-NGINX Controller for Kubernetes	Сетевой	ACE	2023-10-30	✓
17	Критическая	CVE-2023-46747	BIG-IP	Сетевой	ACE	2023-10-26	✓

1

Краткое описание: Обход безопасности в INEA ME RTU

Идентификатор уязвимости: CVE-2023-29155

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: INEA ME RTU: 3.36b

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2023-11-01 / 2023-11-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-304-02

2

Краткое описание: Выполнение произвольного кода в INEA ME RTU

Идентификатор уязвимости: CVE-2023-35762

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

Уязвимый продукт: INEA ME RTU: 3.36b

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 9.9 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: 2023-11-01 / 2023-11-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-304-02

3

Краткое описание: Выполнение произвольного кода в Zavio IP Cameras

Идентификатор уязвимости: CVE-2023-4249

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

Уязвимый продукт: Zavio IP Cameras:
CF7500: M2.1.6.05
CF7300: M2.1.6.05
CF7201: M2.1.6.05
CF7501: M2.1.6.05
CB3211: M2.1.6.05
CB3212: M2.1.6.05
CB5220: M2.1.6.05
CB6231: M2.1.6.05
B8520: M2.1.6.05
B8220: M2.1.6.05
CD321: M2.1.6.05

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-11-01 / 2023-11-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-304-03

4

Краткое описание: Выполнение произвольного кода в Zavio IP Cameras

Идентификатор уязвимости: CVE-2023-39435

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Zavio IP Cameras:
CF7500: M2.1.6.05
CF7300: M2.1.6.05
CF7201: M2.1.6.05
CF7501: M2.1.6.05
CB3211: M2.1.6.05
CB3212: M2.1.6.05
CB5220: M2.1.6.05
CB6231: M2.1.6.05
B8520: M2.1.6.05
B8220: M2.1.6.05
CD321: M2.1.6.05

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

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

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: 2023-11-01 / 2023-11-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-304-03

5

Краткое описание: Выполнение произвольного кода в Zavio IP Cameras

Идентификатор уязвимости: CVE-2023-43755

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Zavio IP Cameras:
CF7500: M2.1.6.05
CF7300: M2.1.6.05
CF7201: M2.1.6.05
CF7501: M2.1.6.05
CB3211: M2.1.6.05
CB3212: M2.1.6.05
CB5220: M2.1.6.05
CB6231: M2.1.6.05
B8520: M2.1.6.05
B8220: M2.1.6.05
CD321: M2.1.6.05

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-01 / 2023-11-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-304-03

6

Краткое описание: Выполнение произвольного кода в Zavio IP Cameras

Идентификатор уязвимости: CVE-2023-45225

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Zavio IP Cameras:
CF7500: M2.1.6.05
CF7300: M2.1.6.05
CF7201: M2.1.6.05
CF7501: M2.1.6.05
CB3211: M2.1.6.05
CB3212: M2.1.6.05
CB5220: M2.1.6.05
CB6231: M2.1.6.05
B8520: M2.1.6.05
B8220: M2.1.6.05
CD321: M2.1.6.05

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-01 / 2023-11-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-304-03

7

Краткое описание: Выполнение произвольного кода в Zavio IP Cameras

Идентификатор уязвимости: CVE-2023-3959

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Zavio IP Cameras:
CF7500: M2.1.6.05
CF7300: M2.1.6.05
CF7201: M2.1.6.05
CF7501: M2.1.6.05
CB3211: M2.1.6.05
CB3212: M2.1.6.05
CB5220: M2.1.6.05
CB6231: M2.1.6.05
B8520: M2.1.6.05
B8220: M2.1.6.05
CD321: M2.1.6.05

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-01 / 2023-11-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-304-03

8

Краткое описание: Перезапись произвольных файлов в Confluence Server and Data Center

Идентификатор уязвимости: CVE-2023-22518

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Confluence Server and Data Center: 6.0.1 - 8.6.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-31 / 2023-10-31

Ссылки на источник:

- http://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-confluence-server-1311473907.html

Краткое описание: Выполнение произвольного кода в Atlassian Sourcetree for Windows

Идентификатор уязвимости: CVE-2023-22514

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Atlassian Sourcetree for Windows: 3.4.14
Atlassian Sourcetree for macOS: 4.2.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

9

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-10-31 / 2023-10-31

Ссылки на источник:

- http://jira.atlassian.com/browse/SRCTREE-8076

Краткое описание: Выполнение произвольного кода в Contec SolarView Compact

Идентификатор уязвимости: CVE-2023-46509

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

Уязвимый продукт: Contec SolarView Compact: 6.00

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-30 / 2023-10-30

Ссылки на источник:

- http://gist.github.com/ATonysan/d6f72e9eb90407d64bed4566aa80afb1#file-cve-2023-46509

Краткое описание: Выполнение произвольного кода в D-Link DAR-7000

Идентификатор уязвимости: CVE-2023-42406

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

Уязвимый продукт: D-Link DAR-7000: 31R02B1413C

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

11

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-30 / 2023-10-30

Ссылки на источник:

- http://github.com/flyyue2001/cve/blob/main/D-LINK%20-DAR-7000_sql_:sysmanage:editrole.php.md
- http://github.com/1dreamGN/CVE/blob/main/CVE-2023-42406.md

12

Краткое описание: Перезапись произвольных файлов в Post Meta Data Manager plugin for WordPress

Идентификатор уязвимости: CVE-2023-5426

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Post Meta Data Manager plugin for WordPress: 1.0.0 - 1.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2023-10-30 / 2023-10-30

Ссылки на источник:

- http://plugins.trac.wordpress.org/changeset/2981559/post-meta-data-manager
- http://www.wordfence.com/threat-intel/vulnerabilities/id/d6a7f882-4582-4b08-9597-329d140ad782?source=cve

13

Краткое описание: Повышение привилегий в Post Meta Data Manager plugin for WordPress

Идентификатор уязвимости: CVE-2023-5425

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Post Meta Data Manager plugin for WordPress: 1.0.0 - 1.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий

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: 2023-10-30 / 2023-10-30

Ссылки на источник:

- http://plugins.trac.wordpress.org/changeset/2981559/post-meta-data-manager
- http://www.wordfence.com/threat-intel/vulnerabilities/id/d7f4e710-99a2-49df-a513-725e1daaa18a?source=cve

14

Краткое описание: Получение конфиденциальной информации в Ingress-NGINX Controller for Kubernetes

Идентификатор уязвимости: CVE-2022-4886

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Ingress-NGINX Controller for Kubernetes: 1.0.0 - 1.7.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 8.8 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: 2023-10-30 / 2023-10-30

Ссылки на источник:

- http://github.com/kubernetes/ingress-nginx/issues/10570
- http://groups.google.com/g/kubernetes-security-announce/c/ge7u3qCwZLI
- http://www.openwall.com/lists/oss-security/2023/10/25/5

15

Краткое описание: Выполнение произвольного кода в Ingress-NGINX Controller for Kubernetes

Идентификатор уязвимости: CVE-2023-5044

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

Уязвимый продукт: Ingress-NGINX Controller for Kubernetes: 1.0.0 - 1.8.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-30 / 2023-10-30

Ссылки на источник:

- http://github.com/kubernetes/ingress-nginx/issues/10572
- http://groups.google.com/g/kubernetes-security-announce/c/ukuYYvRNel0
- http://www.openwall.com/lists/oss-security/2023/10/25/3

16

Краткое описание: Выполнение произвольного кода в Ingress-NGINX Controller for Kubernetes

Идентификатор уязвимости: CVE-2023-5043

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

Уязвимый продукт: Ingress-NGINX Controller for Kubernetes: 1.0.0 - 1.8.4

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-30 / 2023-10-30

Ссылки на источник:

- http://github.com/kubernetes/ingress-nginx/issues/10571
- http://groups.google.com/g/kubernetes-security-announce/c/pVsXsOpxYZo
- http://www.openwall.com/lists/oss-security/2023/10/25/4
- https://bdu.fstec.ru/vul/2023-07144

Краткое описание: Выполнение произвольного кода в BIG-IP

Идентификатор уязвимости: CVE-2023-46747

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: BIG-IP:
17.1.0.3 + Hotfix-BIGIP-17.1.0.3.0.75.4-ENG3
16.1.4.1 + Hotfix-BIGIP-16.1.4.1.0.50.5-ENG3
15.1.10.2 + Hotfix-BIGIP-15.1.10.2.0.44.2-ENG3
14.1.5.6 + Hotfix-BIGIP-14.1.5.6.0.10.6-ENG3
13.1.5.1 + Hotfix-BIGIP-13.1.5.1.0.20.2-ENG3

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

17

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: 2023-10-26 / 2023-10-26

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-46747
- https://my.f5.com/manage/s/article/K000137353