НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-07-18.1 | 18 июля 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-36755	Siemens RUGGEDCOM ROX devices	Сетевой	ACE	2023-07-17	✓
2	Критическая	CVE-2023-36754	Siemens RUGGEDCOM ROX devices	Сетевой	ACE	2023-07-17	✓
3	Критическая	CVE-2023-36753	Siemens RUGGEDCOM ROX devices	Сетевой	ACE	2023-07-17	✓
4	Критическая	CVE-2023-36752	Siemens RUGGEDCOM ROX devices	Сетевой	ACE	2023-07-17	✓
5	Критическая	CVE-2023-36751	Siemens RUGGEDCOM ROX devices	Сетевой	ACE	2023-07-17	✓
6	Критическая	CVE-2023-36750	RUGGEDCOM ROX RX5000	Сетевой	ACE	2023-07-17	✓
7	Высокая	CVE-2023-36390	Siemens RUGGEDCOM ROX devices	Сетевой	XSS\CSS	2023-07-17	✓
8	Высокая	CVE-2023-36389	Siemens RUGGEDCOM ROX devices	Сетевой	XSS\CSS	2023-07-17	✓
9	Высокая	CVE-2023-36386	Siemens RUGGEDCOM ROX devices	Сетевой	XSS\CSS	2023-07-17	✓
10	Высокая	CVE-2023-36887	Microsoft Edge	Локальный	ACE	2023-07-16	✓
11	Высокая	CVE-2023-3596	Rockwell Automation ControlLogix EtherNet/IP (ENIP) communication modules	Сетевой	DoS	2023-07-15	✓
12	Критическая	CVE-2023-3595	Rockwell Automation ControlLogix EtherNet/IP (ENIP) communication modules	Сетевой	ACE	2023-07-15	✓

13	Критическая	CVE-2023-38203	Adobe ColdFusion	Сетевой	ACE	2023-07-15	✓
14	Высокая	CVE-2023-37946	Jenkins OpenShift Login plugin	Сетевой	SUI	2023-07-14	✓
15	Высокая	CVE-2023-24474	Honeywell Experion PKS, LX and PlantCruise	Сетевой	ACE	2023-07-14	✓
16	Высокая	CVE-2023-22435	Honeywell Experion PKS, LX and PlantCruise	Сетевой	ACE	2023-07-14	✓
17	Критическая	CVE-2023-25178	Honeywell Experion PKS, LX and PlantCruise	Сетевой	ACE	2023-07-14	✓
18	Критическая	CVE-2023-25770	Honeywell Experion PKS, LX and PlantCruise	Сетевой	ACE	2023-07-14	✓
19	Критическая	CVE-2023-24480	Honeywell Experion PKS, LX and PlantCruise	Сетевой	ACE	2023-07-14	✓
20	Высокая	CVE-2023-26597	Honeywell Experion PKS, LX and PlantCruise	Сетевой	DoS	2023-07-14	✓
21	Высокая	CVE-2023-25948	Honeywell Experion PKS, LX and PlantCruise	Сетевой	OSI	2023-07-14	✓
22	Критическая	CVE-2023-25078	Honeywell Experion PKS, LX and PlantCruise	Сетевой	ACE	2023-07-14	✓
23	Критическая	CVE-2023-23585	Honeywell Experion PKS, LX and PlantCruise	Сетевой	ACE	2023-07-14	✓
24	Не определено	None	Zimbra Collaboration	Не определено	XSS\CSS	2023-07-13	✗

1

Краткое описание: Выполнение произвольного кода в Siemens RUGGEDCOM ROX devices

Идентификатор уязвимости: CVE-2023-36755

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

Уязвимый продукт: Siemens RUGGEDCOM ROX devices:
RUGGEDCOM ROX RX5000: до 2.16.0
RUGGEDCOM ROX RX1536: до 2.16.0
RUGGEDCOM ROX RX1524: до 2.16.0
RUGGEDCOM ROX RX1512: до 2.16.0
RUGGEDCOM ROX RX1511: до 2.16.0
RUGGEDCOM ROX RX1510: до 2.16.0
RUGGEDCOM ROX RX1501: до 2.16.0
RUGGEDCOM ROX RX1500: до 2.16.0
RUGGEDCOM ROX RX1400: до 2.16.0
RUGGEDCOM ROX MX5000RE: до 2.16.0
RUGGEDCOM ROX MX5000: до 2.16.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-17 / 2023-07-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-146325.txt

2

Краткое описание: Выполнение произвольного кода в Siemens RUGGEDCOM ROX devices

Идентификатор уязвимости: CVE-2023-36754

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

Уязвимый продукт: Siemens RUGGEDCOM ROX devices:
RUGGEDCOM ROX RX5000: до 2.16.0
RUGGEDCOM ROX RX1536: до 2.16.0
RUGGEDCOM ROX RX1524: до 2.16.0
RUGGEDCOM ROX RX1512: до 2.16.0
RUGGEDCOM ROX RX1511: до 2.16.0
RUGGEDCOM ROX RX1510: до 2.16.0
RUGGEDCOM ROX RX1501: до 2.16.0
RUGGEDCOM ROX RX1500: до 2.16.0
RUGGEDCOM ROX RX1400: до 2.16.0
RUGGEDCOM ROX MX5000RE: до 2.16.0
RUGGEDCOM ROX MX5000: до 2.16.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-17 / 2023-07-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-146325.txt

3

Краткое описание: Выполнение произвольного кода в Siemens RUGGEDCOM ROX devices

Идентификатор уязвимости: CVE-2023-36753

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

Уязвимый продукт: Siemens RUGGEDCOM ROX devices:
RUGGEDCOM ROX RX5000: до 2.16.0
RUGGEDCOM ROX RX1536: до 2.16.0
RUGGEDCOM ROX RX1524: до 2.16.0
RUGGEDCOM ROX RX1512: до 2.16.0
RUGGEDCOM ROX RX1511: до 2.16.0
RUGGEDCOM ROX RX1510: до 2.16.0
RUGGEDCOM ROX RX1501: до 2.16.0
RUGGEDCOM ROX RX1500: до 2.16.0
RUGGEDCOM ROX RX1400: до 2.16.0
RUGGEDCOM ROX MX5000RE: до 2.16.0
RUGGEDCOM ROX MX5000: до 2.16.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-17 / 2023-07-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-146325.txt

4

Краткое описание: Выполнение произвольного кода в Siemens RUGGEDCOM ROX devices

Идентификатор уязвимости: CVE-2023-36752

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

Уязвимый продукт: Siemens RUGGEDCOM ROX devices:
RUGGEDCOM ROX RX5000: до 2.16.0
RUGGEDCOM ROX RX1536: до 2.16.0
RUGGEDCOM ROX RX1524: до 2.16.0
RUGGEDCOM ROX RX1512: до 2.16.0
RUGGEDCOM ROX RX1511: до 2.16.0
RUGGEDCOM ROX RX1510: до 2.16.0
RUGGEDCOM ROX RX1501: до 2.16.0
RUGGEDCOM ROX RX1500: до 2.16.0
RUGGEDCOM ROX RX1400: до 2.16.0
RUGGEDCOM ROX MX5000RE: до 2.16.0
RUGGEDCOM ROX MX5000: до 2.16.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-17 / 2023-07-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-146325.txt

5

Краткое описание: Выполнение произвольного кода в Siemens RUGGEDCOM ROX devices

Идентификатор уязвимости: CVE-2023-36751

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

Уязвимый продукт: Siemens RUGGEDCOM ROX devices:
RUGGEDCOM ROX RX5000: до 2.16.0
RUGGEDCOM ROX RX1536: до 2.16.0
RUGGEDCOM ROX RX1524: до 2.16.0
RUGGEDCOM ROX RX1512: до 2.16.0
RUGGEDCOM ROX RX1511: до 2.16.0
RUGGEDCOM ROX RX1510: до 2.16.0
RUGGEDCOM ROX RX1501: до 2.16.0
RUGGEDCOM ROX RX1500: до 2.16.0
RUGGEDCOM ROX RX1400: до 2.16.0
RUGGEDCOM ROX MX5000RE: до 2.16.0
RUGGEDCOM ROX MX5000: до 2.16.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-17 / 2023-07-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-146325.txt

6

Краткое описание: Выполнение произвольного кода в RUGGEDCOM ROX RX5000

Идентификатор уязвимости: CVE-2023-36750

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

Уязвимый продукт: RUGGEDCOM ROX RX5000: до 2.16.0
RUGGEDCOM ROX RX1536: до 2.16.0
RUGGEDCOM ROX RX1524: до 2.16.0
RUGGEDCOM ROX RX1512: до 2.16.0
RUGGEDCOM ROX RX1511: до 2.16.0
RUGGEDCOM ROX RX1510: до 2.16.0
RUGGEDCOM ROX RX1501: до 2.16.0
RUGGEDCOM ROX RX1500: до 2.16.0
RUGGEDCOM ROX RX1400: до 2.16.0
RUGGEDCOM ROX MX5000RE: до 2.16.0
RUGGEDCOM ROX MX5000: до 2.16.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-17 / 2023-07-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-146325.txt

7

Краткое описание: Межсайтовый скриптинг в Siemens RUGGEDCOM ROX devices

Идентификатор уязвимости: CVE-2023-36390

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: Siemens RUGGEDCOM ROX devices:
RUGGEDCOM ROX RX5000: до 2.16.0
RUGGEDCOM ROX RX1536: до 2.16.0
RUGGEDCOM ROX RX1524: до 2.16.0
RUGGEDCOM ROX RX1512: до 2.16.0
RUGGEDCOM ROX RX1511: до 2.16.0
RUGGEDCOM ROX RX1510: до 2.16.0
RUGGEDCOM ROX RX1501: до 2.16.0
RUGGEDCOM ROX RX1500: до 2.16.0
RUGGEDCOM ROX RX1400: до 2.16.0
RUGGEDCOM ROX MX5000RE: до 2.16.0
RUGGEDCOM ROX MX5000: до 2.16.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-17 / 2023-07-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-146325.txt

8

Краткое описание: Межсайтовый скриптинг в Siemens RUGGEDCOM ROX devices

Идентификатор уязвимости: CVE-2023-36389

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: Siemens RUGGEDCOM ROX devices:
RUGGEDCOM ROX RX5000: до 2.16.0
RUGGEDCOM ROX RX1536: до 2.16.0
RUGGEDCOM ROX RX1524: до 2.16.0
RUGGEDCOM ROX RX1512: до 2.16.0
RUGGEDCOM ROX RX1511: до 2.16.0
RUGGEDCOM ROX RX1510: до 2.16.0
RUGGEDCOM ROX RX1501: до 2.16.0
RUGGEDCOM ROX RX1500: до 2.16.0
RUGGEDCOM ROX RX1400: до 2.16.0
RUGGEDCOM ROX MX5000RE: до 2.16.0
RUGGEDCOM ROX MX5000: до 2.16.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-17 / 2023-07-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-146325.txt

9

Краткое описание: Межсайтовый скриптинг в Siemens RUGGEDCOM ROX devices

Идентификатор уязвимости: CVE-2023-36386

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: Siemens RUGGEDCOM ROX devices:
RUGGEDCOM ROX RX5000: до 2.16.0
RUGGEDCOM ROX RX1536: до 2.16.0
RUGGEDCOM ROX RX1524: до 2.16.0
RUGGEDCOM ROX RX1512: до 2.16.0
RUGGEDCOM ROX RX1511: до 2.16.0
RUGGEDCOM ROX RX1510: до 2.16.0
RUGGEDCOM ROX RX1501: до 2.16.0
RUGGEDCOM ROX RX1500: до 2.16.0
RUGGEDCOM ROX RX1400: до 2.16.0
RUGGEDCOM ROX MX5000RE: до 2.16.0
RUGGEDCOM ROX MX5000: до 2.16.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-17 / 2023-07-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-146325.txt

10

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-36887

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 114.0.1823.67

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-16 / 2023-07-16

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36887

Краткое описание: Отказ в обслуживании в Rockwell Automation ControlLogix EtherNet/IP (ENIP) communication modules

Идентификатор уязвимости: CVE-2023-3596

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Rockwell Automation ControlLogix EtherNet/IP (ENIP) communication modules:
1756-EN4TR Series A до 5.002
1756-EN4TRK Series A до 5.002
1756-EN4TRXT Series A до 5.002

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-15 / 2023-07-15

Ссылки на источник:

- http://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140010
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-193-01

12

Краткое описание: Выполнение произвольного кода в Rockwell Automation ControlLogix EtherNet/IP (ENIP) communication modules

Идентификатор уязвимости: CVE-2023-3595

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Rockwell Automation ControlLogix EtherNet/IP (ENIP) communication modules:
1756-EN2T Series A до 5.009
1756-EN2T Series B до 5.009
1756-EN2T Series C до 5.009
1756-EN2T Series D до 11.004
1756-EN2TK Series A до 5.009
1756-EN2TK Series B до 5.009
1756-EN2TK Series C до 5.009
1756-EN2TK Series D до 11.004
1756-EN2TXT Series A до 5.009
1756-EN2TXT Series B до 5.009
1756-EN2TXT Series C до 5.009
1756-EN2TXT Series D до 11.004
1756-EN2TP Series A до 11.004
1756-EN2TPK Series A до 11.004
1756-EN2TPXT Series A до 11.004
1756-EN2TR Series A до 5.009
1756-EN2TR Series B до 5.009
1756-EN2TR Series C до 11.004
1756-EN2TRK Series A до 5.009
1756-EN2TRK Series B до 5.029
1756-EN2TRK Series C до 11.004
1756-EN2TRXT Series A до 5.009
1756-EN2TRXT Series C до 11.004
1756-EN2F Series A до 5.009
1756-EN2TRK Series B до 5.029
1756-EN2F Series C до 11.004
1756-EN2FK Series A до 5.009
1756-EN2FK Series C до 11.004
1756-EN3TR Series A до 5.029

1756-EN3TR Series B до 11.004
1756-EN3TRK Series A до 5.029
1756-EN3TRK Series B до 11.004

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-15 / 2023-07-15

Ссылки на источник:

- http://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140010
- http://www.bleepingcomputer.com/news/security/rockwell-warns-of-new-apt-rce-exploit-targeting-critical-infrastructure/
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-193-01

13

Краткое описание: Выполнение произвольного кода в Adobe ColdFusion

Идентификатор уязвимости: CVE-2023-38203

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Adobe ColdFusion: 2018 - 2023 Update 1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-15 / 2023-07-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/coldfusion/apsb23-41.html

Краткое описание: Пользовательский интерфейс подмены в Jenkins OpenShift Login plugin

Идентификатор уязвимости: CVE-2023-37946

Идентификатор программной ошибки: CWE-384 Фиксация сессии

Уязвимый продукт: Jenkins OpenShift Login plugin: 1.1.0.227.v27e08dfb_1a_20 - 1.1.0.227.v27e08dfb_1a_20

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Пользовательский интерфейс подмены

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-14 / 2023-07-14

Ссылки на источник:

- http://jenkins.io/security/advisory/2023-07-12/

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, LX and PlantCruise

Идентификатор уязвимости: CVE-2023-24474

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

Уязвимый продукт: Honeywell Experion PKS, LX and PlantCruise:
Experion PKS до R520.2
Experion LX до R520.2
Experion PlantCruise до R520.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-14 / 2023-07-14

Ссылки на источник:

- http://process.honeywell.com
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-194-06

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, LX and PlantCruise

Идентификатор уязвимости: CVE-2023-22435

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

Уязвимый продукт: Honeywell Experion PKS, LX and PlantCruise:
Experion PKS до R520.2
Experion LX до R520.2
Experion PlantCruise до R520.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-14 / 2023-07-14

Ссылки на источник:

- http://process.honeywell.com
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-194-06

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, LX and PlantCruise

Идентификатор уязвимости: CVE-2023-25178

Идентификатор программной ошибки: CWE-345 Некорректная проверка достоверности данных

Уязвимый продукт: Honeywell Experion PKS, LX and PlantCruise:
Experion PKS до R520.2
Experion LX до R520.2
Experion PlantCruise до R520.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-14 / 2023-07-14

Ссылки на источник:

- http://process.honeywell.com
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-194-06

18

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, LX and PlantCruise

Идентификатор уязвимости: CVE-2023-25770

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Honeywell Experion PKS, LX and PlantCruise:
Experion PKS до R520.2
Experion LX до R520.2
Experion PlantCruise до R520.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-14 / 2023-07-14

Ссылки на источник:

- http://process.honeywell.com

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, LX and PlantCruise

Идентификатор уязвимости: CVE-2023-24480

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Honeywell Experion PKS, LX and PlantCruise:
Experion PKS до R520.2
Experion LX до R520.2
Experion PlantCruise до R520.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-14 / 2023-07-14

Ссылки на источник:

- http://process.honeywell.com
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-194-06

Краткое описание: Отказ в обслуживании в Honeywell Experion PKS, LX and PlantCruise

Идентификатор уязвимости: CVE-2023-26597

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

Уязвимый продукт: Honeywell Experion PKS, LX and PlantCruise:
Experion PKS до R520.2
Experion LX до R520.2
Experion PlantCruise до R520.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-14 / 2023-07-14

Ссылки на источник:

- http://process.honeywell.com
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-194-06

Краткое описание: Получение конфиденциальной информации в Honeywell Experion PKS, LX and PlantCruise

Идентификатор уязвимости: CVE-2023-25948

Идентификатор программной ошибки: CWE-394 Непредусмотренные коды состояния или возвращаемые значения

Уязвимый продукт: Honeywell Experion PKS, LX and PlantCruise:
Experion PKS до R520.2
Experion LX до R520.2
Experion PlantCruise до R520.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-14 / 2023-07-14

Ссылки на источник:

- http://process.honeywell.com
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-194-06

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, LX and PlantCruise

Идентификатор уязвимости: CVE-2023-25078

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Honeywell Experion PKS, LX and PlantCruise:
Experion PKS до R520.2
Experion LX до R520.2
Experion PlantCruise до R520.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-14 / 2023-07-14

Ссылки на источник:

- http://process.honeywell.com
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-194-06

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, LX and PlantCruise

Идентификатор уязвимости: CVE-2023-23585

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

Уязвимый продукт: Honeywell Experion PKS, LX and PlantCruise:
Experion PKS до R520.2
Experion LX до R520.2
Experion PlantCruise до R520.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-14 / 2023-07-14

Ссылки на источник:

- http://process.honeywell.com
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-194-06

Краткое описание: Межсайтовый скриптинг в Zimbra Collaboration

Идентификатор уязвимости: None

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: Zimbra Collaboration: 8.8.15 - 8.8.15 Patch 40

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Межсайтовый скриптинг

24 **Рекомендации по устранению:** Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

Оценка CVSSv3: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://info.zimbra.com/security-update-zimbra-collaboration-suite-version-8.8.15-important
- http://twitter.com/maddiestone/status/1679542322772721664