НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200319.4 | 19 марта 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ПО коммутаторов компании Moxa

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	MOXA AWK-3131A v1.13
Дата выявления (обновления)	25 февраля 2020 г. (27 февраля 2020 г.)

Идентификаторы		Описание уязвимости, ссылки на источники	Оценка CVSSv3.1
Уязвимость	Программная ошибка		
MITRE: CVE-2019-5138	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в оболочке целевой системы посредством отправки специально сформированных команд во время аутентификации в качестве пользователя с низким уровнем привилегий. Уязвимость обусловлена некорректной проверкой входных данных в компоненте зашифрованного диагностического сценария. https://talosintelligence.com/vulnerability_reports/TALOS-2019-0927 Рекомендации по устранению: обновить программное обеспечение	9.9

MITRE: CVE-2019-5136	CWE-269: Некорректное управление привилегиями	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код от имени пользователя root в целевой системе посредством отправки специальных команд во время аутентификации в качестве пользователя с низким уровнем привилегий. Уязвимость обусловлена некорректной работой компонента iw_console. https://talosintelligence.com/vulnerability_reports/TALOS-2019-0925 Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2019-5140	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в уязвимом устройстве посредством создания диагностического скрипта с определённым именем файла и отображения в следующем вызове функции iw_system введенных пользователем данных. Уязвимость обусловлена некорректной работой компонента микропрограммы iw_webs. https://talosintelligence.com/vulnerability_reports/TALOS-2019-0929 Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2019-5141	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в уязвимом устройстве посредством отправки специальных команды во время аутентификации в качестве пользователя с низким уровнем привилегий. Уязвимость обусловлена некорректной работой специально созданного параметра iw_serverip и отображения в следующем вызове iw_system введенных пользователем данных. https://talosintelligence.com/vulnerability_reports/TALOS-2019-0930 Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2019-5142	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)	Эксплуатация уязвимости позволяет удаленному злоумышленнику внедрить вредоносный SQL-код в уязвимое устройство посредством отправки различных аутентификационных запросов. Уязвимость обусловлена некорректной фильтрации данных, передаваемых и извлекаемых из флэш-памяти. https://talosintelligence.com/vulnerability_reports/TALOS-2019-0931 Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2019-5143	CWE-134: Использование форматной строки, контролируемой извне	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код вредоносный SQL-код в уязвимое устройство посредством отправки команды во время аутентификации в качестве пользователя с низким	8.8

		уровнем привилегий. Уязвимость обусловлена некорректной обработкой параметров при настройке сервера времени. https://talosintelligence.com/vulnerability_reports/TALOS-2019-0932 Рекомендации по устранению: обновить программное обеспечение	
MITRE: CVE-2019-5148	CWE-191: Потеря значимости целых чисел (простой или циклический возврат)	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством копирования большого объема данных. Уязвимость обусловлена некорректной обработкой параметров при настройке сервера времени. https://talosintelligence.com/vulnerability_reports/TALOS-2019-0938 Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2019-5137	CWE-798: Использование жестко закодированных учетных данных	Эксплуатация уязвимости позволяет удаленному злоумышленнику расшифровывать захваченный сетевой трафик в целевом устройстве. Уязвимость обусловлена некорректной работой жестко закодированных криптографических ключей. https://talosintelligence.com/vulnerability_reports/TALOS-2019-0926 Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE: CVE-2019-5139	CWE-798: Использование жестко закодированных учетных данных	Эксплуатация уязвимости позволяет удаленному злоумышленнику создать собственные диагностические сценарии для обработки в целевом устройстве посредством загрузки этих сценариев через портал устранения неполадок устройства. Уязвимость обусловлена наличием недокументированного пароля (moxaiwroot) используемого при расшифровке любых диагностических сценариев. https://talosintelligence.com/vulnerability_reports/TALOS-2019-0928 Рекомендации по устранению: обновить программное обеспечение	7.1

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020022406?affChecked=1 https://www.moxa.com/en/support/support/security-advisory/awk-3131a-series-industrial-ap-bridge-client-vulnerabilities