НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220204.4 | 4 февраля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости Cisco RV340 Dual WAN Gigabit VPN Router

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco RV340 Dual WAN Gigabit VPN Router: 1.0.0.33, 1.0.03.18, 1.0.03.19, 1.0.03.20, 1.0.03.21, 1.0.03.22, 1.0.03.24, 1.0.1.16, 1.0.3.17 Cisco RV340W Dual WAN Gigabit Wireless-AC VPN Router: 1.0.01.16, 1.0.01.17, 1.0.01.18, 1.0.01.20, 1.0.02.16, 1.0.03.15, 1.0.03.16, 1.0.03.17, 1.0.03.18, 1.0.03.19, 1.0.03.20, 1.0.03.21, 1.0.03.22, 1.0.03.24 Cisco RV345 Dual WAN Gigabit VPN Router: 1.0.0.33, 1.0.03.18, 1.0.03.19, 1.0.03.20, 1.0.03.21, 1.0.03.22, 1.0.03.24, 1.0.1.16, 1.0.3.17 Cisco RV345P Dual WAN Gigabit VPN Router: 1.0.0.33, 1.0.03.24, 1.0.1.16
Дата выявления	3 февраля 2022 г.
Дата обновления	3 февраля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-20712	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	9.8

	CWE-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: обновить программное обеспечение	
MITRE: CVE-2022-20711	Эксплуатация уязвимости позволяет удаленному злоумышленнику перезаписывать произвольные файлы в системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение	8.2
MITRE: CVE-2022-20709	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально сформированного HTTP-запроса на загрузку файла. Уязвимость обусловлена некорректной проверкой файла во время загрузки. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-434: Отсутствие ограничений на загрузку файлов небезопасного типа Рекомендации по устранению: обновить программное обеспечение	10.0
MITRE: CVE-2022-20749 CVE-2022-20707	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: обновить программное обеспечение	7.3

MITRE: CVE-2022-20708	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: обновить программное обеспечение	10.0
MITRE: CVE-2022-20706	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной проверкой входных данных в модуле Open Plug and Play (PnP). CVSSv3.0: AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: обновить программное обеспечение	8.3
MITRE: CVE-2022-20705	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации и получить доступ к веб-интерфейсу целевой системы посредством подбора идентификатора сеанса. Уязвимость обусловлена ошибкой в функции генерации идентификатора сеанса. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-287: Некорректная аутентификация Рекомендации по устранению: обновить программное обеспечение	9.0
MITRE: CVE-2022-20703	Эксплуатация уязвимости позволяет злоумышленнику с физическим доступом к устройству скомпрометировать уязвимую систему. Уязвимость обусловлена некорректной проверкой криптографической подписи образов программного обеспечения при их установке на уязвимое устройство. CVSSv3.0: AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-347: Некорректная проверка криптографической подписи	7.6

	Рекомендации по устранению: обновить программное обеспечение	
MITRE: CVE-2022-20702	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена отсутствием авторизации в веб-интерфейсе управления. CVSSv3.0: AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-285: Некорректная авторизация Рекомендации по устранению: обновить программное обеспечение	8.2
MITRE: CVE-2022-20701	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена отсутствием авторизации в веб-интерфейсе управления. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-285: Некорректная авторизация Рекомендации по устранению: обновить программное обеспечение	10.0
MITRE: CVE-2022-20700	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена отсутствием авторизации в веб-интерфейсе управления. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-285: Некорректная авторизация Рекомендации по устранению: обновить программное обеспечение	10.0

Ссылки на источники	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-mult-vuln-KA9PK6D https://www.cybersecurity-help.cz/vdb/SB2022020301