НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200727.4 | 27 июля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco RV340, RV340W, RV345, RV345P Dual WAN Gigabit VPN Routers

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco RV340 Dual WAN Gigabit VPN Router: -, 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 Cisco RV345 Dual WAN Gigabit VPN Router: -, 1.0.3.17 Cisco RV345P Dual WAN Gigabit POE VPN Router: -, 1.0.3.17
Дата выявления	15 июля 2020 г.
Дата обновления	22 июля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-3357	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных компонентом SSL VPN. CVSS:3.0 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.	9.8

MITRE: CVE-2020-3358	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании у целевой системы посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных компонентом SSL VPN. CVSS:3.0 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.	8.6
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-dos-ZN5GvNH7 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rce-dos-9ZAjkx4	