НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200508.1 | 8 мая 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Adaptive Security Appliance (ASA) и Firepower Threat Defense (FTD)

Категория уязвимого продукта	Средства защиты информации
Уязвимое ПО	Cisco Adaptive Security Appliance (ASA) до v9.14 Cisco Firepower Threat Defense (FTD) до v6.6.0
Дата выявления	6 мая 2020 г.
Дата обновления	7 мая 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-3187	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным на целевом устройстве посредством отправки специально созданного вредоносного HTTP-запроса. Уязвимость обусловлена недостаточной проверкой корректности предоставленного пользователем URL-адреса в HTTP-запросе. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) Рекомендации по устранению: обновить программное обеспечение.	9.1

MITRE: CVE-2020-3195	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально сформированных вредоносных OSPF-пакетов. Уязвимость обусловлена некорректной реализацией механизма обработки сетевых пакетов по протоколу Open Shortest Path First (OSPF) в программном обеспечении ASA и FTD. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов) Рекомендации по устранению: обновить программное обеспечение.	8.6
MITRE: CVE-2020-3298	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки серии специально сформированных вредоносных OSPF-пакетов за короткий промежуток времени. Уязвимость обусловлена некорректной реализацией механизма защиты памяти приложений при обработке сетевых пакетов по протоколу Open Shortest Path First (OSPF) в программном обеспечении ASA и FTD. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: обновить программное обеспечение.	8.6
MITRE: CVE-2020-3196	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством установки нескольких SSL/TLS соединений с определенными параметрами. Уязвимость обусловлена некорректной реализацией механизма управления ресурсами для входящих SSL/TLS соединений. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов) Рекомендации по устранению: обновить программное обеспечение.	8.6

MITRE: CVE-2020-3191	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально сформированного вредоносного DNS-пакета по протоколу IPv6. Уязвимость обусловлена некорректной проверкой длины поля в DNS-пакете отправленного по протоколу IPv6. CVSSv3.0: 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
MITRE: CVE-2020-3254	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально созданных вредоносных пакетов по протоколу Media Gateway Control (MGCP) через уязвимое устройство. Уязвимость обусловлена некорректной работой функции проверки протокола MGCP. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов) Рекомендации по устранению: обновить программное обеспечение.	8.6
MITRE: CVE-2020-3179	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально созданных вредоносных пакетов Generic Routing Encapsulation (GRE) по протоколу IPv6 через уязвимое устройство. Уязвимость обусловлена ошибкой памяти при обработке GRE-пакетов по протоколу IPv6. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-415: Двойное освобождение Рекомендации по устранению: обновить программное обеспечение.	8.6

MITRE: CVE-2020-3259	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным на целевом устройстве посредством отправки специально сформированного GET запроса. Уязвимость обусловлена некорректным отслеживанием границ буфера памяти при обработке недействительных URL-адресов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-200: Разглашение информации Рекомендации по устранению: обновить программное обеспечение.	7.5

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ospf-memleak-DHpsgfnv https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ospf-dos-RhMQY8qx https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssl-vpn-dos-qY7BHpjN https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ipv6-67pA658k https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-path-JE3azWw43 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-mgcp-SUqB8VKH https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-2-sS2h7aWe