НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201030.9 | 30 октября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco ASA и FTD

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco ASA до v9.14.1.30, 9.13.1.13, 9.12.4.4, 9.10.1.44, 9.9.2.80, 9.8.4.29, 9.6.4.45 Cisco FTD от v6.2.2 до v6.6.1
Дата выявления	21 октября 2020 г.
Дата обновления	21 октября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-3304	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления. 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-2020-3529	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного DTLS трафика. Уязвимость обусловлена некорректным управлением памятью при создании SSL VPN-соединения. 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-2020-3528	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного сетевого пакета. Уязвимость обусловлена некорректной проверкой OSPFv2-пакетов с данными локальной сигнализации (LLS). 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-2020-3373	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного IP-фрагмента. Уязвимость обусловлена некорректной обработкой возникших ошибок при повторных сборках IP-фрагментов. 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-2020-3436	Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить произвольные файлы в локальные директории и вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена некорректной обработкой процесса записи файлов большого размера в систему. 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-434: Отсутствие ограничений на загрузку файлов небезопасного типа Рекомендации по устранению: обновить программное обеспечение.	8.6

MITRE: CVE-2020-3554	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного сетевого пакета. Уязвимость обусловлена некорректной обработкой TCP-пакетов. 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-434: Отсутствие ограничений на загрузку файлов небезопасного типа Рекомендации по устранению: обновить программное обеспечение.	8.6
MITRE: CVE-2020-3572	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством создания и закрытия нескольких SSL/TLS сеансов. Уязвимость обусловлена некорректным распределением памяти при завершении SSL/TLS соединения. 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

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webdos-fBzM5Ynw https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-sslvpndma-dos-HRrqB9Yx https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ospflls-37Xy2q6r https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-frag-memleak-mCtqdP9n https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-fileup-dos-zvC7wtys https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-QFcNEPfx https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-tcp-dos-N3DMnU4T