НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201106.4 | 6 ноября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco SD-WAN Software

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Cisco SD-WAN Software версии ПО до 18.4, 19.2, 19.3, 20.1, 20.3
Дата выявления	4 ноября 2020 г.
Дата обновления	4 ноября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-3595 CVE-2020-3593 CVE-2020-3600 CVE-2020-3594 CVE-2020-26074	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить привилегии в целевой системе посредством отправки специально сформированного запроса приложению. Уязвимость обусловлена некорректным применением настроек безопасности. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-269: Некорректное управление привилегиями CWE-250: Выполнение операций с избыточными привилегиями Рекомендации по устранению: обновить программное обеспечение.	7.8

MITRE: CVE-2020-26073	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированных запросов к API приложения. Уязвимость обусловлена некорректной проверкой входных данных. 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-35: Выход за пределы каталога с помощью '.../...//' Рекомендации по устранению: обновить программное обеспечение.	7.5
MITRE: CVE-2020-26071	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного запроса приложению. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H/E:U/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) Рекомендации по устранению: обновить программное обеспечение.	8.4

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepegr-4xynYLUj https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepescm-BjgQm4vJ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepeshlg-tJghOQcA https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepestd-8C3J9Vc https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-traversal-hQh24tmk https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-escalation-Jhqs5Skf https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vsoln-arbfile-gtsEYxns