НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ
VULN-20201125.13 | 25 ноября 2020
Уровень опасности: КРИТИЧЕСКИЙ
Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Security Manager

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Security Manager до v4.22
Дата выявления	16 ноября 2020 г.
Дата обновления	17 ноября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-27130	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной проверкой последовательностей символов обхода каталога в запросах к уязвимому устройству. 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-35: Выход за пределы каталога с помощью '.../...//' Рекомендации по устранению: обновить программное обеспечение.	9.1

MITRE: CVE-2020-27131	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код с привилегиями «NT AUTHORITY\SYSTEM» в целевой системе посредством отправки специально созданного вредоносного сетевого пакета. Уязвимость обусловлена некорректной работой функции десериализации. CVSSv3.0: AV:N/AC:H/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.	8.1
MITRE: CVE-2020-27125	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством использования жестко закодированных учетных данных в прошивке уязвимого продукта. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-798: Использование жестко закодированных учетных данных Рекомендации по устранению: обновить программное обеспечение.	7.4
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-path-trav-NgeRnqgR https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-java-rce-mWJEedcD https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-rce-8gjUz9fW	