НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210203.9 | 3 февраля 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Smart Software Manager Satellite

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Релизы Cisco Smart Software Manager On-Prem (Cisco Smart Software Manager Satellite) до v6.3.0
Дата выявления	20 января 2021 г.
Дата обновления	20 января 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-1138 CVE-2021-1140 CVE-2021-1142	Эксплуатация уязвимостей позволяет удалённому злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных вредоносных HTTP-запросов. Уязвимость обусловлена некорректной обработкой входных данных в веб-интерфейсе управления Cisco Smart Software Manager Satellite. CVSSv3.1: 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-2021-1139 CVE-2021-1141	Эксплуатация уязвимостей позволяет удалённому аутентифицированному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных вредоносных HTTP-запросов. Уязвимость обусловлена некорректной обработкой входных данных в веб-интерфейсе управления Cisco Smart Software Manager Satellite. CVSSv3.0: AV:N/AC:L/PR:L/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.	8.8

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A