



НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210722.2 | 22 июля 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Cisco Intersight Virtual Appliance

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Intersight Virtual Appliance: до v1.0.9-292
Дата выявления	22 июля 2021 г.
Дата обновления	22 июля 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-1600 CVE-2021-1601	<p>Эксплуатация уязвимости позволяет злоумышленнику из смежной сети получить несанкционированный доступ к данным в целевой системе посредством отправки специально сформированных вредоносных сетевых пакетов на интерфейс управления. Уязвимость обусловлена некорректной обработкой IPv4 или IPv6 пакетов на внешнем интерфейсе управления.</p> <p>CVSSv3.0: AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-284: Некорректное управление доступом</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.3

<p>MITRE: CVE-2021-1618</p>	<p>Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных данных в веб-интерфейсе управления. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления.</p> <p>CVSSv3.0: AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C</p> <p>CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>7.2</p>
<p>Ссылки на источники</p>	<p>https://www.cybersecurity-help.cz/vdb/SB2021072230 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsi2-dtcinj-yH5U4RSx https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsi2-iptaclbp-L8Dzs8m8</p>	