

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201203.1 | 3 декабря 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Удаленное выполнение кода в Trend Micro InterScan Web Security Virtual Appliance

Идентификатор уязвимости	MITRE: CVE-2020-28578
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной обработкой входных данных в веб-интерфейсе управления.
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	Trend Micro IWSVA до v6.5 SP2 Hotfix 1919
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	18 ноября 2020 г.
Дата обновления	29 ноября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)

Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-28578 https://success.trendmicro.com/solution/000281954