

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200907.5 | 7 сентября 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Несанкционированный доступ в Trend Micro Vulnerability Protection

Идентификатор уязвимости	MITRE: CVE-2020-15601 CVE-2020-15605
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к уязвимому приложению посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной обработкой запросов аутентификации, если включена LDAP-аутентификация.
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	Trend Micro Vulnerability Protection до v2.0 SP2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	29 июля 2020 г.
Дата обновления	29 июля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
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://www.cybersecurity-help.cz/vdb/SB2020083112>
<https://success.trendmicro.com/solution/000252039>
<https://www.zerodayinitiative.com/advisories/ZDI-20-1077/>
<https://www.zerodayinitiative.com/advisories/ZDI-20-1083/>