НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210927.4 | 27 сентября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Обход аутентификации в Trend Micro ServerProtect

Идентификатор уязвимости	MITRE: CVE-2021-36745
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректным процессом аутентификации.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	ServerProtect: 5.8, 6.0 ServerProtect for Storage (SPFS): 6.0 ServerProtect for EMC Celerra (SPEMC): 5.8 ServerProtect for Network Appliance Filers (SPNAF): 5.8 ServerProtect for Microsoft Windows / Novell Netware (SPNT): 5.8
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	24 сентября 2021 г.
Дата обновления	24 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
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://www.cybersecurity-help.cz/vdb/SB2021092403 https://success.trendmicro.com/solution/000289038