НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210302.3 | 2 марта 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в VMware ESXi

Идентификатор уязвимости	MITRE: CVE-2020-21974
Идентификатор программной ошибки	Не определен
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику, находящемуся в смежной сети, выполнить произвольный код в целевой системе посредством отправки специально сформированных сетевых пакетов на порт 427. Уязвимость обусловлена некорректным функционированием компонента OpenSLP. Серверное программное обеспечение и его компоненты
Уязвимый продукт	ESXi: версия 6.5 до ESXi650-202102101-SG версия 6.7 до ESXi670-202102401-SG версия 7.0 до ESXi70U1c-17325551 Cloud Foundation (ESXi): версия 3.x до 3.10.1.2 версия 4.x до 4.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	23 февраля 2021 г.
Дата обновления	23 февраля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Смежная сеть (A)
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.vmware.com/security/advisories/VMSA-2021-0002.html