НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201231.6 | 31 декабря 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд API в Orion Platform

Идентификатор уязвимости	MITRE: CVE-2020-10148
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации и выполнить произвольные команды API посредством отправки специально сформированного запроса на сервер. Уязвимость обусловлена некорректной обработкой запросов на аутентификацию в SolarWinds Orion API.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Orion Platform: 2016.1, 2016.2, 2017.1, 2017.3, 2017.3 HF 3, 2017.3 HF 4, 2017.3 HF 5, 2018.2, 2018.2 HF 2, 2018.2 HF 3, 2018.2 HF 4, 2018.2 HF 5, 2018.2 HF 6, 2018.4, 2018.4 HF 1, 2018.4 HF 2, 2018.4 HF 3, 2019.2, 2019.2 HF 1, 2019.2 HF 2, 2019.2 HF 3, 2019.4, 2019.4 HF 1, 2019.4 HF 2, 2019.4 HF 3, 2019.4 HF 4, 2019.4 HF 5, 2020.2, 2020.2 HF 1, 2020.2.1, 2020.2.1 HF 1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	28 декабря 2020 г.
Дата обновления	28 декабря 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	10.0 AV:N/AC:L/PR:N/UI:N/S:C/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)	Изменяется (C)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Высокая
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020122801 https://www.kb.cert.org/vuls/id/843464 https://www.solarwinds.com/securityadvisory