

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230213.4 | 13 февраля 2023 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Повышение привилегий в PC Settings Tool

Идентификатор уязвимости	MITRE: CVE-2023-25011
Идентификатор программной ошибки	CWE-306: Отсутствие аутентификации для критически важных функций
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной работой механизма безопасности проверяющего подлинность запроса.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	PC Settings Tool: до 11.0.23.0
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	10 февраля 2023 г.
Дата обновления	10 февраля 2023 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с	Отсутствует (N)

пользователем (UI)

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

Не определено

Наличие средств устранения уязвимости

Официальное решение

Достоверность сведений об уязвимости

Не определено

Ссылки на источники

<http://jvn.jp/en/jp/JVN60320736/index.html>