НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200605.11 | 5 июня 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Получение полного доступа в SWARCO CPU LS4000

Идентификатор уязвимости	MITRE: CVE-2020-12493
Идентификатор программной ошибки	CWE-284: Некорректное управление доступом
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить полный доступ к целевой системе посредством подключения к сетевому порту, предназначенному для отладки целевого устройства. Уязвимость обусловлена некорректной работой механизма разграничения доступа.
Категория уязвимого продукта	Промышленное программно-аппаратное оборудование
Уязвимое ПО	CPU LS4000 с ПО vG4
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	28 мая 2020 г.
Дата обновления	2 июня 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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://cert.vde.com/de-de/advisories/vde-2020-016 https://nvd.nist.gov/vuln/detail/CVE-2020-12493