НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200127.1 | 23 января 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Обход аутентификации на маршрутизаторе Genexis Platinum

Идентификатор уязвимости	MITRE: CVE-2020-6170
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить аутентификационные данные для доступа к панели администрирования маршрутизатора путём просмотра исходного HTML кода страницы авторизации.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Genexis Platinum-4410 P4410-V2–1.28
Рекомендации по устранению	Отсутствуют
Дата выявления	8 января 2020 г.
Дата обновления	24 января 2020 г.
Оценка критичности уязвимости (CVSSv3)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:X/RC:C
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 (E)	Функциональная версия (F)
Наличие средств устранения уязвимости (RL)	Не определено (X)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://packetstormsecurity.com/files/156075/Genexis-Platinum-4410-2.1-Authentication-Bypass.html https://medium.com/@husinulzsanub/exploiting-router-authentication-through-web-interface-68660c708206