НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200507.1 | 7 мая 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Внедрение SQL-команд в GLPI

Идентификатор уязвимости	MITRE: CVE-2020-11032
Идентификатор программной ошибки	CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (Внедрение SQL-кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные SQL-запросы к базе данных приложения. Уязвимость обусловлена недостаточной очисткой предоставленных пользователем данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	GLPI до v9.4.6
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 мая 2020 г.
Дата обновления	5 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.6 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Высокий (H)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Низкое (L)

Влияние на доступность (A)	Отсутствует (N)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-11032 https://github.com/glpi-project/glpi/security/advisories/GHSA-344w-34h9-wwhh