НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230413.4 | 13 апреля 2023 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в GLPI

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	GLPI: 0.83 - 0.90.5, 9.1 - 9.5.12, 10.0.0 - 10.0.6
Дата выявления	7 апреля 2023 г.
Дата обновления	7 апреля 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-28634	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректной авторизацией. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-285: Некорректная авторизация 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.	8.8

MITRE: CVE-2023-28632	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректное управление привилегиями CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N CWE-269: Некорректное управление привилегиями 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.	8.1
MITRE: CVE-2023-28838	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных уязвимого приложения посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода) 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.	9.6
MITRE: CVE-2023-28849	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных уязвимого приложения посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)	10.0

	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.	

Ссылки на источники	http://github.com/glpi-project/glpi/security/advisories/GHSA-2c7r-gf38-358f http://github.com/glpi-project/glpi/security/advisories/GHSA-9r84-jpg3-h4m6 http://github.com/glpi-project/glpi/releases/tag/10.0.7 http://github.com/glpi-project/glpi/releases/tag/9.5.13 http://github.com/glpi-project/glpi/security/advisories/GHSA-7pwm-pg76-3q9x http://github.com/glpi-project/glpi/security/advisories/GHSA-4279-rxmh-gf39