НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191218.1 | 18 декабря 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Некорректная проверка входных данных в ПО Cacti

Идентификатор уязвимости	MITRE: CVE-2019-17358
Идентификатор программной ошибки	CWE-502: Десериализация недоверенных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику вызвать отказ в обслуживании приложения в целевой системе путем отправки специально созданных вредоносных пакетов. Уязвимость обусловлена некорректной проверкой входных данных в модуле functions.php.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Cacti до v1.2.7
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 декабря 2019 г.
Дата обновления	12 декабря 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Высокое (H)

Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Концептуальное подтверждение (P)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://github.com/Cacti/cacti/commit/adf221344359f5b02b8aed43dfb6b33ae5d708c8 https://nvd.nist.gov/vuln/detail/CVE-2019-17358 https://bugzilla.suse.com/show_bug.cgi?id=CVE-2019-17358