НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191230.3 | 30 декабря 2019 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в ПО Odoo

Идентификатор уязвимости	MITRE: CVE-2019-11780
Идентификатор программной ошибки	CWE-269: Некорректное управление привилегиями CWE-284: Некорректное управление доступом
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить привилегии в целевой системе посредством отправки специально сформированных RPC-запросов. Уязвимость обусловлена некорректной обработкой несохраненных вычисляемых полей от имени суперпользователя.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Odoo Community Edition 13.0 Odoo Enterprise Edition 13.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 декабря 2019 г.
Дата обновления	27 декабря 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:U/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)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Отсутствует (N)
Степень зрелости доступных средств эксплуатации (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)

Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2019-11780 https://github.com/odoo/odoo/issues/42196