НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200602.4| 2 июня 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Выполнение произвольных команд в пакете Python jw.util

Идентификатор уязвимости	MITRE: CVE-2020-13388
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять произвольные команды в целевой системе посредством отправки специально сформированного вредоносного сетевого пакета. Уязвимость обусловлена некорректной проверкой обрабатываемых YAML-файлов при загрузке конфигурации.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	jw.util v2.3
Рекомендации по устранению	На данный момент отсутствуют
Дата выявления	22 мая 2020 г.
Дата обновления	28 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
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	Концептуальное подтверждение
Наличие средств устранения уязвимости	Отсутствует
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-13388 https://joel-malwarebenchmark.github.io/