НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201030.4 | 30 октября 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Oracle Healthcare Foundation

Идентификатор уязвимости	MITRE: CVE-2020-1953
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного файла. Уязвимость обусловлена некорректной конфигурацией сторонней библиотеки для разбора YAML-файлов.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Apache Commons Configuration: v2.2, v2.3, v2.4, v2.5, v2.6 Oracle Healthcare Foundation v7.1.1, v7.2.0, v7.2.1, v7.3.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	13 марта 2020 г.
Дата обновления	20 октября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	10.0 AV:N/AC:L/PR:N/UI:N/S:C/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)	Изменяется (C)
Влияние на конфиденциальность (C)	Высокое (H)

Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.oracle.com/security-alerts/cpuoct2020.html https://www.oracle.com/security-alerts/cpuoct2020verbose.html https://nvd.nist.gov/vuln/detail/CVE-2020-1953 https://www.cybersecurity-help.cz/vdb/SB2020102303