# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200303.1 | 3 марта 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

## Несанкционированный доступ к данным в ПО Apache Tomcat

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2020-1938 |
| Идентификатор программной ошибки | CWE-20: Некорректная проверка входных данных |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным на уязвимом сервере, а если данный сервер поддерживает загрузку файлов, то и выполнить произвольный код посредством отправки специально сформированного вредоносного пакета по протоколу Apache JServ Protocol (AJP). Уязвимость обусловлена некорректной работой AJP-коннектора. |
| Категория уязвимого продукта | Серверное программное обеспечение и его компоненты |
| Уязвимое ПО | Apache Tomcat: v7.0.0 до v7.0.99, v8.5.0 до v8.5.50, v9.0.0.M1 до v9.0.0.30 и v6.x |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 24 февраля 2020 г. |
| Дата обновления | 27 февраля 2020 г. |
| Оценка критичности уязвимости (CVSSv3.0) | 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/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) | 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 (E) | Концептуальное подтверждение (P) |
| 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-2020-1938<br>http://tomcat.apache.org/security-9.html<br>http://tomcat.apache.org/security-8.html<br>http://tomcat.apache.org/security-7.html |