

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220727.18 | 27 июля 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

НСД в Questions For Confluence app for Confluence Server and Data Center

Идентификатор уязвимости	MITRE: CVE-2022-26138
Идентификатор программной ошибки	CWE-506: Внедренный вредоносный код
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена жестко закодированной учетной записью.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Questions for Confluence: 2.7.34 - 2.7.35, 3.0.2
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	25 июля 2022 г.
Дата обновления	25 июля 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
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	Высокая
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены

Ссылки на источники

<http://confluence.atlassian.com/doc/confluence-security-advisory-2022-07-20-1142446709.html>
<http://jira.atlassian.com/browse/CONFSERVER-79483>