НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220901.24 | 1 сентября 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд оболочки в Bitbucket Server и Data Center

Идентификатор уязвимости	MITRE: CVE-2022-36804
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Bitbucket Server: 7.0.1 - 7.0.5, 7.1.0 - 7.1.4, 7.2.0 - 7.2.6, 7.3.0 - 7.3.2, 7.4.0 - 7.4.2, 7.5.0 - 7.5.2, 7.6.0 - 7.6.16, 7.7.0 - 7.7.1, 7.8.0 - 7.8.1, 7.9.0 - 7.9.1, 7.10.0 - 7.10.1, 7.11.1 - 7.11.2, 7.12.0 - 7.12.1, 7.13.0 - 7.13.1, 7.14.0 - 7.14.2, 7.15.0 - 7.15.3, 7.16.0 - 7.16.3, 7.17.0 - 7.17.9, 7.18.0 - 7.18.4, 7.19.0 - 7.19.5, 7.20.0 - 7.20.3, 7.21.0 - 7.21.3, 8.0.0 - 8.0.2, 8.1.0 - 8.1.2, 8.2.0 - 8.2.1, 8.3.0 Bitbucket Server and Data Center: 7.0.1 - 7.0.5, 7.1.0 - 7.1.4, 7.2.0 - 7.2.6, 7.3.0 - 7.3.2, 7.4.0 - 7.4.2, 7.5.0 - 7.5.2, 7.6.0 - 7.6.16, 7.7.0 - 7.7.1, 7.8.0 - 7.8.1, 7.9.0 - 7.9.1, 7.10.0 - 7.10.1, 7.11.1 - 7.11.2, 7.12.0 - 7.12.1, 7.13.0 - 7.13.1, 7.14.0 - 7.14.2, 7.15.0 - 7.15.3, 7.16.0 - 7.16.3, 7.17.0 - 7.17.9, 7.18.0 - 7.18.4, 7.19.0 - 7.19.5, 7.20.0 - 7.20.3, 7.21.0 - 7.21.3, 8.0.0 - 8.0.2, 8.1.0 - 8.1.2, 8.2.0 - 8.2.1, 8.3.0
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	29 августа 2022 г.
Дата обновления	29 августа 2022 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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	http://jira.atlassian.com/browse/BSERV-13438 http://confluence.atlassian.com/bitbucketserver/bitbucket-server-and-data-center-advisory-2022-08-24-1155489835.html