НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211203.4 | 3 декабря 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Jenkins и Jenkins LTS

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Jenkins: до 2.318 Jenkins LTS: до 2.303.2
Дата выявления	8 ноября 2021 г.
Дата обновления	8 ноября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-21690	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректной политикой безопасности. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-693: Некорректное использование защитных механизмов Рекомендации по устранению: обновить программное обеспечение	9.8

MITRE: CVE-2021-21693	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс авторизации и создать произвольные файлы в целевой системе. Уязвимость обусловлена некорректной проверкой разрешений на создание файлов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-285: Некорректная авторизация Рекомендации по устранению: обновить программное обеспечение	9.8
MITRE: CVE-2021-21697	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс авторизации, прочитать и записать содержимое каталогов в уязвимом приложении. Уязвимость обусловлена отсутствием авторизации. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:L/E:U/RL:O/RC:C CWE-862: Отсутствие авторизации Рекомендации по устранению: обновить программное обеспечение	8.9
MITRE: CVE-2021-21689 CVE-2021-21691	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс авторизации, прочитать и записать произвольные файлы в целевой системе. Уязвимость обусловлена отсутствием авторизации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-862: Отсутствие авторизации Рекомендации по устранению: обновить программное обеспечение	9.8

MITRE: CVE-2021-21688	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс авторизации и прочитать произвольные файлы. Уязвимость обусловлена отсутствием авторизации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-862: Отсутствие авторизации Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE: CVE-2021-21692	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс авторизации и записать произвольные файлы. Уязвимость обусловлена отсутствием авторизации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-862: Отсутствие авторизации Рекомендации по устранению: обновить программное обеспечение	9.8
MITRE: CVE-2021-21696	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством подмены файлов доверенной библиотеки на вредоносные. Уязвимость обусловлена некорректными ограничениями безопасности. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-693: Некорректное использование защитных механизмов Рекомендации по устранению: обновить программное обеспечение	8.8

MITRE: CVE-2021-21685	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс авторизации, прочитать и записать произвольные файлы в целевой системе. Уязвимость обусловлена отсутствием авторизации. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-862: Отсутствие авторизации Рекомендации по устранению: обновить программное обеспечение	9.0
MITRE: CVE-2021-21695	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс авторизации и прочитать произвольные файлы в целевой системе посредством перехода по символическим ссылкам. Уязвимость обусловлена отсутствием авторизации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-862: Отсутствие авторизации Рекомендации по устранению: обновить программное обеспечение	9.8
MITRE: CVE-2021-21686	Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать произвольный файлы в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) Рекомендации по устранению: обновить программное обеспечение	7.5

MITRE: CVE-2021-21694	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение	9.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021113017 http://jenkins.io/security/advisory/2021-11-04/