НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211206.2 | 6 декабря 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в IBM Cloud Pak System

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	IBM Cloud Pak System: до 2.3.3.3 iFix 1
Дата выявления	3 декабря 2021 г.
Дата обновления	3 декабря 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-21985	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение	9.8

MITRE: CVE-2021-21991	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректной обработкой токена сеанса. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/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	8.8
MITRE: CVE-2021-22006	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой систем посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной обработкой URI. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/RC:C CWE-285: Некорректная авторизация Рекомендации по устранению: обновить программное обеспечение	8.3
MITRE: CVE-2021-22009	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректным использованием ресурсов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов) Рекомендации по устранению: обновить программное обеспечение	8.6

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021120331 http://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-vmware-vcenter-affect-ibm-cloud-pak-system-2/ http://www.ibm.com/support/pages/node/6507111