

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220906.7 | 6 сентября 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в IBM Netezza Host Management

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	IBM Netezza Host Management: до 5.4.31.0
Дата выявления	2 сентября 2022 г.
Дата обновления	2 сентября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-25215	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена возможностью вызова утверждения при обработке записей DNAME.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C</p> <p>CWE-617: Несанкционированный вызов утверждения</p> <p>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.</p>	7.5

MITRE: CVE-2020-8625	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C</p> <p>CWE-119: Выполнение операций за пределами буфера памяти</p> <p>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.</p>	8.1
-------------------------	--	-----

Ссылки на источники	<p>http://www.ibm.com/support/pages/node/6490827</p> <p>http://www.ibm.com/blogs/psirt/security-bulletin-publicly-disclosed-vulnerabilities-from-bind-affect-ibm-netezza-host-management-4/</p>
---------------------	---