

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230215.4 | 15 февраля 2023 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Microsoft SQL Server

Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Microsoft SQL Server: 2014 12.0.2000.8 - 2022 RC1 16.0.950.9
Дата выявления	14 февраля 2023 г.
Дата обновления	15 февраля 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-21704	<p>Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-20: Некорректная проверка входных данных</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>	7.8

MITRE: CVE-2023-21568	<p>Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику вызвать отказ в обслуживании целевой системы посредством открытия пользователем специально созданного файла. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H</p> <p>CWE-20: Некорректная проверка входных данных</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>	7.3
MITRE: CVE-2023-21705	<p>Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-20: Некорректная проверка входных данных</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>	8.8
MITRE: CVE-2023-21528	<p>Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-20: Некорректная проверка входных данных</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>	7.8

<p>MITRE: CVE-2023-21713</p>	<p>Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-20: Некорректная проверка входных данных</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>	<p>8.8</p>
<p>MITRE: CVE-2023-21718</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством подключения пользователя к базе данных вредоносного SQL-сервера. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H</p> <p>CWE-20: Некорректная проверка входных данных</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>	<p>7.8</p>

Ссылки на
источники

<http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21705>
<http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21718>
<http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21568>
<http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21528>
<http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21704>
<http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21713>