НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200226.2 | 26 февраля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в ПО Microsoft SQL Server

Идентификатор уязвимости	MITRE: CVE-2020-0618
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному в программе злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного HTTP-запроса. Уязвимость обусловлена некорректной работой метода OnLoad в ReportingServicesWebServer.dll.
Категория уязвимого продукта	Серверное программное обеспечение
Уязвимое ПО	Microsoft SQL Server 2012 for 32-bit Systems SP 4 (QFE) Microsoft SQL Server 2012 for x64-based Systems SP 4 (QFE) Microsoft SQL Server 2014 SP 3 for 32-bit Systems (CU) Microsoft SQL Server 2014 SP 3 for 32-bit Systems (GDR) Microsoft SQL Server 2014 SP 3 for x64-based Systems (CU) Microsoft SQL Server 2014 SP 3 for x64-based Systems (GDR) Microsoft SQL Server 2016 for x64-based Systems SP 2 (CU) Microsoft SQL Server 2016 for x64-based Systems SP 2 (GDR)
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	11 февраля 2020 г.
Дата обновления	13 февраля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)

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 (E)	Концептуальное подтверждение (P)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618 https://www.tenable.com/blog/cve-2020-0618-proof-of-concept-for-microsoft-sql-server-reporting-services-vulnerability-0 https://www.mdsec.co.uk/2020/02/cve-2020-0618-rce-in-sql-server-reporting-services-ssrs/