GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

28 August 2026

Advisory 203: CVE-2019-1068 - Microsoft SQL Server Remote Code Execution Vulnerability

Release Date: 26th August 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

Any organisation operating Microsoft SQL Server. In Vanuatu this includes government agencies running line-of-business and records systems, banking and financial institutions, telecommunications operators and Internet Service Providers, and any organisation whose web or business applications are backed by a SQL Server database.

What is it?

CVE-2019-1068 is a remote code execution vulnerability in Microsoft SQL Server, carrying a CVSS v3.0 Base Score of 8.8 (vector AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). It arises from incorrect handling of the processing of internal functions, and takes the form of a stack-based memory corruption flaw within the database engine.

An attacker who is able to authenticate to the database, at any privilege level, can submit a specially crafted query and execute arbitrary code in the context of the SQL Server Database Engine service account. Microsoft addressed the issue on 9 July 2026.

What are the systems affected?

Microsoft SQL Server installations that have not received the July 2019 security update or a later GDR or Cumulative Update package - (Affected)

Installations updated to the fixed GDR or Cumulative Update build for their version, or later - (Not affected, patched)

Organisations should confirm the affected versions and the correct update package for their deployment against the Microsoft Security Update Guide entry for CVE-2019-1068, which is the authoritative source.

What does this mean?

Exploitation requires the attacker to be able to authenticate to the database. This is a genuine limitation, but it is a lower barrier in practice than it may appear, and there are several routes to it that do not require the attacker to hold a legitimate account.

Web applications hold database credentials in their configuration files, so an attacker who compromises a public-facing application generally obtains valid database credentials as a matter of course. A SQL injection flaw in an application provides authenticated query execution directly. Any ordinary internal user with a database login, including a reporting or read-only account, is also in a position to exploit the flaw.

The consequence is determined by the account under which the database engine runs. Code executes with the privileges of the SQL Server Database Engine service account. Where that account is a dedicated low-privilege identity, the compromise is largely confined to the database host.

Mitigation process

CERTVU recommends the following:

1. **Identify SQL Server Instances and Their Patch Level**

Inventory all SQL Server instances, including those installed as components of third-party business applications, which are frequently overlooked. Determine the build number of each instance and compare it against the fixed build in the Microsoft Security Update Guide.

```
SELECT @@VERSION;
SELECT SERVERPROPERTY('ProductVersion'),
SERVERPROPERTY('ProductLevel');
```

2. **Apply the Security Update**

Apply the appropriate GDR or Cumulative Update package for each instance.

Other mitigating options include;

- Review the Database Engine Service Account
- Restrict Database Network Exposure and Accounts
- Migrate Unsupported Versions
- Review for Prior Compromise

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2019-1068
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-1068

4. https://nvd.nist.gov/vuln/detail/CVE-2019-1068