EXPLOITED VULNERABILITY ADVISORY: CVE-2019-1068

Summary

CVE-2019-1068 in Microsoft SQL Server is being actively exploited in the wild. A remote code execution vulnerability exists in Microsoft SQL Server when it incorrectly handles processing of internal functions, aka 'Microsoft SQL Server Remote Code Execution Vulnerability'. CISA requires federal remediation by 2026-08-29; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2019-1068
- **Affected:** Microsoft SQL Server
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-26
- **Severity:** CVSS 8.8 High, Network-exploitable, no user interaction (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 53%

Recommended action

Patch CVE-2019-1068 by 2026-08-29. If you cannot patch immediately, limit network exposure of the affected service and tighten access until patched. If you ship an affected product, be ready to file the CRA 24-hour report the moment you find it exploited.

Sources: CISA Known Exploited Vulnerabilities, NIST NVD. Public data; an advisory of active exploitation, not an incident report. Verify applicability to your estate before acting.