CVE-2020-0618

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-0618
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-11 22:15:00 UTC
Updated	2022-01-01 19:59:00 UTC
Description	A remote code execution vulnerability exists in Microsoft SQL Server Reporting Services when it incorrectly handles page r

Risk And Classification

EPSS: 0.942520000 probability, percentile 0.999330000 (date 2026-05-14)

CISA KEV: Listed on 2024-09-18; due 2024-10-09; ransomware use Unknown

Problem Types: CWE-502

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	SQL Server
Name	Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0618 ; https://nvd.nist.gov/vuln/detail/CVE-2020-0618

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Sql Server	2012	sp4	All	All
Application	Microsoft	Sql Server	2014	sp3	All	All
Application	Microsoft	Sql Server	2016	sp2	All	All
Application	Microsoft	Sql Server	2012	sp4	All	All
Application	Microsoft	Sql Server	2014	sp3	All	All
Application	Microsoft	Sql Server	2016	sp2	All	All

References

References

Reference	Source	Link	Tags
Microsoft SQL Server Reporting Services 2016 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618	MISC	portal.msrc.microsoft.com	Patch, Ve
SQL Server Reporting Services (SSRS) ViewState Deserialization ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**