

CVE-2023-7101

Spreadsheet::ParseExcel Remote Code Execution Vulnerability

CISA KEV since Jan 2, 2024

Actively exploited

Public exploit module (Metasploit)

Spreadsheet::ParseExcel version 0.65 is a Perl module used for parsing Excel files. Spreadsheet::ParseExcel is vulnerable to an arbitrary code execution (ACE) vulnerability due to passing unvalidated input from a file into a string-type "eval". Specifically, the issue stems from the evaluation of Number format strings (not to be confused with printf-style format strings) within the Excel parsing logic.

EVRS 75/100 Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.190 97.3rd percentile · FIRST	CISA DEADLINE Jan 23, 2024 KEV since 2024 · listed over a year
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.190 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. **CISA**

note: This vulnerability affects a common open-source component, third-party library, or a protocol used by different products.

Please check with specific vendors for information on patching status.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
spreadsheet\	\ ≤ 0.65	no fixed version listed	NVD
debian linux	10.0	no fixed version listed	NVD
fedora	38 39	no fixed version listed	NVD

Sources

Vendor guidance	https://github.com/jmcnamara/spreadsheet-parseexcel/commit/bd3159277e745468e2c553417b35d5d7dc7405bc	metacpan.org/dist/Spreadsheet-ParseExcel and Barracuda's specific implementation and fix for their downstream issue CVE-2023-7102 at https://www.barracuda.com/company/legal/esg-vulnerability	metacpan.org/dist/Spreadsheet-ParseExcel and Barracuda's specific implementation and fix for their downstream issue CVE-2023-7102 at https://www.barracuda.com/company/legal/esg-vulnerability
NVD	nvd.nist.gov/vuln/detail/CVE-2023-7101	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-59285	Current data	evulnable.com/vulnerability-management/cve/CVE-2023-7101

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.