January 4, 2024

Overall rating: Critical

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Perl-based web apps has been exploited in wild. Attackers can exploit this vulnerability by using specially crafted Number format strings within XLS and XLSX files, triggering the execution of arbitrary code during the parsing process.

Technical Details

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.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-7101
- https://github.com/mandiant/Vulnerability-Disclosures/blob/master/2023/MNDT-2023-0019.md