Heap Memory Corruption With RSA Private Key Operation (CVE-2022-2274)

Advisory Details

Severity

9.8 Critical

Advisory ID

CVE-2022-2274

CVSS Score

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Security Advisory Summary

SolarWinds made aware of the OpenSSL security advisory published on July 5, 2022. The OpenSSL 3.0.4 release introduced a serious bug in the RSA implementation for X86_64 CPUs supporting the AVX512IFMA instructions. This issue makes the RSA implementation with 2048-bit private keys incorrect on such machines, and memory corruption will happen during the computation. Consequently, an attacker may be able to trigger a remote code execution on the machine performing the computation. SSL/TLS servers or other servers using 2048-bit RSA private keys running on machines supporting AVX512IFMA instructions of the X86_64 architecture are affected by this issue.

SolarWinds® products don't use OpenSSL version 3.0.4, which was released on June 21, 2022, and aren't known to be affected by the vulnerability identified in CVE-2022-2274.

For more information on this CVE and guidance to mitigate this vulnerability, please visit the OpenSSL security advisory.