OpenSSL buffer overflows in punycode decoding functions (CVE-2022-3602 and CVE-2022-3786)

Summary

October 25, 2022, the OpenSSL Project announced the forthcoming release of OpenSSL version 3.0.7. to address the vulnerability assessed with the severity of high.

November 1, 2022, the OpenSSL Project released the OpenSSL 3.0.7 version and details about CVE-2022-3602 and CVE-2022-3786 have been released.

SolarWinds investigated all products and infrastructure to identify the versions of OpenSSL utilized. Following our investigation, we have detected the following products and versions that are susceptible to this vulnerability:

- Serv-U 15.3.1

We have confirmed all other SolarWinds products, including the Orion Platform and SolarWinds Platform and their modules, are not known to be affected by this issue, while they might utilize the OpenSSL library.

Affected Products

- OpenSSL 3.0.0 =< OpenSSL 3.0.7

Fixed Software Release

- OpenSSL 3.0.7

Advisory Details

Severity

7.5 High
7.5 High

Advisory ID

- CVE-2022-3602
- CVE-2022-3786

First Published

11/01/2022

Last Updated

11/10/2022

Fixed Version

OpenSSL 3.0.7

CVSS Score

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