Advisory Alert

Alert Number: AAA20230721 **Date:** July 21, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**High**	Out-of-bounds write Vulnerability
OpenSSL	**Low**	Denial of service Vulnerability

Description

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Out-of-bounds write Vulnerability (CVE-2023-35077)
Description	Ivanti has released a patch update to address Out-of-bounds write vulnerability in Ivanti Antivirus antimalware engines on Windows operating systems that causes the engine to crash. Ivanti recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Ivanti Antivirus Security Content version 7.94791 and all previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/SA-2023-07-19-CVE-2023-35077?language=en_US

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Denial of service Vulnerability (CVE-2023-3446)
Description	OpenSSL has released a security updates addressing a Denial of service Vulnerability exists due to improper management of internal resources within the DH_check(), DH_check_ex() and EVP_PKEY_param_check() function when processing a DH key or DH parameters.By using specially crafted data to the application remote attacker can perform a denial of service. OpenSSL recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	OpenSSL 3.1, 3.0, 1.1.1 and 1.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20230719.txt

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.