Advisory Alert

Alert Number: **AAA20230421** **Date:** **April 21, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple Vulnerabilities
Qnap	**High**, **Medium**, **Low**	Multiple Vulnerabilities
OpenSSL	Low	Denial of Service Vulnerability

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20864, CVE-2023-20865)
Description	VMware has released security updates addressing multiple vulnerabilities that exists in the product **CVE-2023-20864** - There is a deserialization vulnerability in VMware Aria Operations for Logs. An unauthenticated attacker could possibly execute arbitrary code as root if they had network access to VMware Aria Operations for Logs. **CVE-2023-20865** - VMware Aria Operations for Logs contains a command injection vulnerability. A malicious actor with administrative privileges in VMware Aria Operations for Logs can execute arbitrary commands as root. VMware highly recommends to apply necessary security fixes to avoid issues.
Affected Products	VMware Aria Operations for Logs (formerly vRealize Log Insight)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0007.html

Affected Product	**Qnap**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3437, CVE-2022-3592, CVE-2022-42898, CVE-2022-27597, CVE-2022-27598, CVE-2023-23355, CVE-2023-22809)
Description	Qnap has released security updates addressing multiple vulnerabilities that exists in their products. Exploitation of these vulnerabilities can leads to buffer overflow, sensitive data exposure, and local attacker to append arbitrary entries to the list of files to process. Qnap recommends to apply necessary security fixes to avoid issues.
Affected Products	QTS, QuTS hero, QuTScloud, QVP (QVR Pro appliances)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-23-02 https://www.qnap.com/en/security-advisory/qsa-23-03 https://www.qnap.com/en/security-advisory/qsa-23-06 https://www.qnap.com/en/security-advisory/qsa-23-10 https://www.qnap.com/en/security-advisory/qsa-23-11

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-1255)
Description	OpenSSL has released a security update addressing a denial of service vulnerability that exists in their products This vulnerability exists due to a boundary error within the AES-XTS cipher decryption implementation for 64 bit ARM platform. An attacker with ability to control the size and location of the ciphertext buffer can trigger an out-of-bounds read and crash the application, leading to denial of service. Due to the low severity of this issue they are not issuing new releases of OpenSSL at this time and also fix is available in commit bc2f61ad (for 3.1) and commit 02ac9c94 (for 3.0) in the OpenSSL git repository
Affected Products	OpenSSL 3.0.0 - 3.0.8 and 3.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20230420.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.