Advisory Alert

Alert Number: **AAA20231113** **Date:** **November 13, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High, Medium**	Multiple Vulnerabilities
Ivanti	**High, Medium**	Multiple Vulnerabilities
NETGEAR	**High, Medium**	Multiple Vulnerabilities
QNAP	**Medium**	OS command injection vulnerability

Description

Affected Product	**IBM**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-22218, CVE-2023-20593, CVE-2023-35788, CVE-2022-44730, CVE-2022-44729, CVE-2023-20900, CVE-2023-3341, CVE-2023-3899, CVE-2023-43057)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products .if exploited these vulnerabilities could lead to denial of service, sensitive information disclosure, privilege escalation. IBM recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	IBM QRadar SIEM 7.5 - 7.5.0 UP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7070736

Affected Product	**Ivanti**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-41718, CVE-2023-35080, CVE-2023-38543, CVE-2023-38043, CVE-2023-38544, CVE-2023-39335, CVE-2023-39337)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. if exploited these vulnerabilities could lead to denial of service, sensitive information disclosure, privilege escalation and compromise the integrity and security of the network on the affected system. Ivanti recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Pulse Desktop Client Ivanti Secure Access Client below 22.5R1 Ivanti Endpoint Manager Mobile (EPMM) Versions 11.10, 11.9 ,11.8 and Older versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/CVE-2023-39337?language=en_US https://forums.ivanti.com/s/article/Security-fixes-included-in-the-latest-Ivanti-Secure-Access-Client-Release?language=en_US https://forums.ivanti.com/s/article/CVE-2023-39335?language=en_US

Affected Product	**NETGEAR**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Netgear has released security updates addressing multiple vulnerabilities that exist in their products. if exploited these vulnerabilities could lead to Pre-authentication Buffer Overflow, denial of service, Security Misconfiguration Netgear recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	NMS300 firmware version before 1.7.0.31 Cable Modem Routers CAX30 firmware versions before 2.2.1.12 RAX30 Routers firmware versions before 1.0.10.94 ReadyNAS OS 6 versions before 6.10.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000065859/Security-Advisory-for-Pre-authentication-Buffer-Overflow-on-the-CAX30-PSV-2023-0093?article=000065859 https://kb.netgear.com/000065860/Security-Advisory-for-Denial-of-Service-on-the-RAX30-PSV-2023-0099?article=000065860 https://kb.netgear.com/000065861/Security-Advisory-for-Improper-Firmware-Signature-Scheme-on-the-RAX30-PSV-2023-0100?article=000065861 https://kb.netgear.com/000065542/Security-Advisory-for-Multiple-Vulnerabilities-on-ReadyNAS-OS-6-PSV-2023-0015-PSV-2023-0016?article=000065542 https://kb.netgear.com/000065866/Security-Advisory-for-Multiple-Vulnerabilities-on-the-NMS300-PSV-2023-0114-PSV-2023-0115?article=000065866

Affected Product	**QNAP**
Severity	**Medium**
Affected Vulnerability	OS command injection vulnerability (CVE-2023-23367)
Description	QNAP has released a security update addressing an OS command injection vulnerability that exist in their products. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network QNAP recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	QTS 5.0.1.2376 before build 20230421 QuTS hero h5.0.x before QuTS hero h5.0.1.2376 build 20230421 QuTScloud c5.x before QuTScloud c5.1.0.2498
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-23-24

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.