Advisory Alert

Alert Number: AAA20230427 **Date:** April 27, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**High**	Service Location Protocol Vulnerability
IBM	**Medium**	Cross-site Scripting Vulnerability

Description

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Service Location Protocol Vulnerability (CVE-2023-29552)
Description	NetApp has released a security update to address a Service Location Protocol vulnerability that exists in the NetApp SMI-S Provider. Using this flow in Service Location Protocol, a remote, unauthenticated attacker could be able to register arbitrary services, enabling them to cause Denial of Service with a significant amplification factor via spoofed UDP traffic. NetApp recommends to apply the necessary workaround at your earliest to avoid issues.
Affected Products	NetApp SMI-S Provider
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20230426-0001/

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Cross-site Scripting Vulnerability (CVE-2023-24966)
Description	IBM has released Security Updates addressing a Cross-site Scripting Vulnerability that exist in IBM WebSphere Application Server and IBM WebSphere Hybrid Edition. Using this vulnerability, attackers can modify embedded arbitrary JavaScript code in the Web UI to alter its intended function and steal potentially sensitive information within a trusted session. IBM recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	IBM WebSphere Application Server 8.5 ,9.0 IBM WebSphere Hybrid Edition 5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6986341 https://www.ibm.com/support/pages/node/6986333

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.