Advisory Alert

Alert Number: **AAA20241202** **Date:** **December 2, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Security Update
Zabbix	**Critical**	SQL injection Vulnerability
NetApp	**High, Medium**	Multiple Vulnerabilities
Zabbix	**High, Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2022-0318)
Description	NetApp has released security update addressing a Vulnerability that exists in their products. **CVE-2022-0318 -** Multiple NetApp products incorporate Vim. Vim versions prior to v8.2.4151 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP tools for VMware vSphere 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20241115-0004/

Affected Product	**Zabbix**
Severity	**Critical**
Affected Vulnerability	SQL injection Vulnerability (CVE-2024-42327)
Description	Zabbix has released security updates addressing a SQL injection Vulnerability that exists in their products. **CVE-2024-42327 -** A non-admin user account on the Zabbix frontend with the default User role, or with any other role that gives API access can exploit this vulnerability. An SQLi exists in the CUser class in the addRelatedObjects function, this function is being called from the CUser.get function which is available for every user who has API access. Zabbix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Zabbix API Versions - 6.0.0-6.0.31, 6.4.0-6.4.16, 7.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.zabbix.com/security_advisories

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0727, CVE-2023-5678, CVE-2024-4741, CVE-2024-4603, CVE-2024-6119, CVE-2024-5535)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products.These vulnerabilities could be exploited by malicious users to cause Denial of Service, Disclosure of Sensitive Information, Addition or Modification of Data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20240208-0006/ • https://security.netapp.com/advisory/ntap-20231130-0010/ • https://security.netapp.com/advisory/ntap-20240621-0004/ • https://security.netapp.com/advisory/ntap-20240621-0001/ • https://security.netapp.com/advisory/ntap-20240912-0001/ • https://security.netapp.com/advisory/ntap-20240712-0005/

Affected Product	**Zabbix**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42333, CVE-2024-42332, CVE-2024-42331, CVE-2024-42330, CVE-2024-42329, CVE-2024-42328, CVE-2024-42326, CVE-2024-36468, CVE-2024-36467, CVE-2024-36466, CVE-2024-36464, CVE-2024-36463, CVE-2024-22117)
Description	Zabbix has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Arbitrary Code Execution, Privilege Escalation, Log Tampering (Forging) Zabbix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Zabbix Server, Proxy Versions - 5.0.0-5.0.42, 6.0.0-6.0.34, 6.4.0-6.4.19, 7.0.0-7.0.3 Zabbix Frontend, API Versions - 5.0.0-5.0.43, 6.0.0-6.0.33, 6.4.0-6.4.18, 7.0.0-7.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.zabbix.com/security_advisories

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.