Advisory Alert

Alert Number: AAA20230911 **Date:** September 11, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NodeJS	**High**, **Medium**, **Low**	Permission Policy Bypass vulnerabilities
NetApp	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**NodeJS**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Permission Policy Bypass vulnerabilities (CVE-2023-32002, CVE-2023-32004, CVE-2023-32558, CVE-2023-32006, CVE-2023-32559, CVE-2023-32005, CVE-2023-32003)
Description	NodeJS has released security update addressing multiple Permission Policy Bypass vulnerabilities affecting v16.x, v18.x, and v20.x Node.js releases. Exploitation of these vulnerabilities could lead to path traversal and Arbitrary Code execution. NodeJS recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	v16.x, v18.x, and v20.x Node.js release
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/august-2023-security-releases#permissions-policies-can-be-bypassed-via-processbinding-mediumcve-2023-32559

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31425, CVE-2023-31426, CVE-2023-31427, CVE-2023-31428, CVE-2023-31429, CVE-2023-31430, CVE-2023-31431, CVE-2023-31432, CVE-2023-31926, CVE-2023-31927, CVE-2023-31928)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Brocade Fabric OS versions prior to 9.2.0, 9.1.1c, and 8.2.3d
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20230908-0007/

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2023-21255, CVE-2023-2163, CVE-2023-35828, CVE-2023-2002, CVE-2023-31084, CVE-2023-3268, CVE-2023-2269, CVE-2023-35824, CVE-2023-35823, CVE-2023-3212, CVE-2023-38426, CVE-2023-2898, CVE-2022-48425, CVE-2023-38428, CVE-2023-38429, CVE-2023-32247, CVE-2023-32250, CVE-2023-32257, CVE-2023-32252, CVE-2023-32258)
Description	Ubuntu has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Denial of service, Sensitive information disclosure and Arbitrary code execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 23.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6340-2 https://ubuntu.com/security/notices/USN-6339-2 https://ubuntu.com/security/notices/USN-6338-2

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.