



Advisory Alert

Alert Number: AAA20240212

Date: February 12, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

| Product | Severity | Vulnerability |
|---------|-------------------------|---|
| Ubuntu | High, Medium, Low | Multiple Vulnerabilities |
| Zabbix | Medium | Improper Input Validation Vulnerability |

Description

| | |
|---------------------------------------|---|
| Affected Product | Ubuntu |
| Severity | High, Medium, Low |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-46813, CVE-2023-6932, CVE-2024-0641, CVE-2023-6931, CVE-2023-6606, CVE-2023-35827, CVE-2024-0193, CVE-2023-32252, CVE-2023-34324, CVE-2023-6040, CVE-2023-32257, CVE-2023-6817, CVE-2023-6176, CVE-2023-32250, CVE-2023-6622, CVE-2023-6039) |
| Description | <p>Ubuntu has released a security update addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Arbitrary Code Execution, Denial of Service, Disclosure of Information</p> <p>Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.</p> |
| Affected Products | Ubuntu 22.04 LTS |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://ubuntu.com/security/notices/USN-6628-1 |

| | |
|---------------------------------------|--|
| Affected Product | Zabbix |
| Severity | Medium |
| Affected Vulnerability | Improper Input Validation Vulnerability (CVE-2024-22119) |
| Description | <p>Zabbix has released a security update addressing an improper input validation vulnerability in their products. By exploiting, malicious code can be entered into the graph item name field, which can be executed when the user clicks on the current graph item name link.</p> <p>Zabbix recommends to apply the necessary patch updates at your earliest to avoid issues.</p> |
| Affected Products | 5.0.0-5.0.39 6.0.0-6.0.23 6.4.0-6.4.8 7.0.0alpha1-7.0.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://support.zabbix.com/browse/ZBX-24070 |

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.