Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

CERT-MU Vulnerability Note VN-2024-2

Multiple Linux Kernel Zero-Day Vulnerabilities

Date of Issue: 28.02.2024

Severity Rating: High

Affected Products:

- Linux Kernel

Description

Linux Kernel could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free within the handling of TCP connection and disconnection. An attacker could exploit this vulnerability to execute arbitrary code on the system.

Solution

Users are advised to apply updates to address the vulnerabilities. Before applying the patch, please visit the vendor website for more details:

- https://git.kernel.org/stable/c/24290ba94cd0136e417283b0dbf8fcdabcf62111
- https://git.kernel.org/stable/c/380965e48e9c32ee4263c023e1d830ea7e462ed1
- https://git.kernel.org/stable/c/38d20c62903d669693a1869aa68c4dd5674e2544
- https://git.kernel.org/stable/c/69d54650b751532d1e1613a4fb433e591aeef126
- https://git.kernel.org/stable/c/999daf367b924fdf14e9d83e034ee0f86bc17ec6

CVE Information

- CVE-2024-26592 CVSS:9
- CVE-2024-26594 CVSS:9.3

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26592
- https://ubuntu.com/security/CVE-2024-26592
- https://nvd.nist.gov/vuln/detail/CVE-2024-26592

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2024-26594
- https://ubuntu.com/security/CVE-2024-26594
- https://nvd.nist.gov/vuln/detail/CVE-2024-26594

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Ministry of Information Technology, Communication and Innovation

Tel: (+230) 4602600
Hotline No: (+230) 800 2378
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org