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

CERT-MU Vulnerability Note

CERT-MU Vulnerability Note VN-2024-12

Multiple Microsoft Products Vulnerabilities

Date of Issue: 27.12.2024

Severity Rating: Medium

Affected Products:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2025 - 10.0.0 - 10.0.0
- Microsoft Windows 10 Version 1809 - 10.0.0
- Microsoft Windows Server 2019 - 10.0.0
- 23H2 Edition (Server Core installation) - 10.0.0
- Microsoft Windows 11 Version 24H2 - 10.0.0 - 10.0.0
- Microsoft Windows Server 2019 (Server Core installation) - 10.0.0
- Microsoft Windows 10 Version 21H2 - 10.0.0
- Microsoft Windows 11 Version 23H2 - 10.0.0
- Microsoft Windows 11 version 22H3 - 10.0.0
- Microsoft Office 2019 - 19.0.0
- Microsoft 365 Apps for Enterprise - 16.0.1
- Microsoft SharePoint Enterprise Server 2016 - 16.0.0
- Microsoft SharePoint Server 2019 - 16.0.0
- Microsoft Microsoft SharePoint Server 2019 - 16.0.0
- Microsoft SharePoint Server Subscription Edition - 16.0.0
- Microsoft Microsoft SharePoint Server Subscription Edition - 16.0.0

Description

Microsoft Office could allow a local attacker to execute arbitrary code on the system. By executing a specially crafted program, an attacker could exploit this vulnerability to execute arbitrary code on the system.

Microsoft SharePoint could allow a remote authenticated attacker to obtain sensitive information. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information.

Solution

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

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49065

CVE Information

- CVE-2024-49065 CVSS:5.5
- CVE-2024-49062 CVSS:6.5
- CVE-2024-49103 CVSS:4.3
- CVE-2024-49101 CVSS:6.6
- CVE-2024-49099 CVSS:4.3
- CVE-2024-49098 CVSS:4.3
- CVE-2024-49094 CVSS:6.6
- CVE-2024-49092 CVSS:6.8
- CVE-2024-49087 CVSS:4.6
- CVE-2024-49073 CVSS:6.8
- CVE-2024-49064 CVSS:6.5

References

- https://nvd.nist.gov/vuln/detail/CVE-2024-49065
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-49065
- https://www.tenable.com/cve/CVE-2024-49065
- https://nvd.nist.gov/vuln/detail/CVE-2024-49062
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-49062
- https://www.tenable.com/cve/CVE-2024-49062
- https://nvd.nist.gov/vuln/detail/CVE-2024-49103
- https://www.tenable.com/cve/CVE-2024-49103
- https://nvd.nist.gov/vuln/detail/CVE-2024-49101
- https://www.tenable.com/cve/CVE-2024-49101
- https://nvd.nist.gov/vuln/detail/CVE-2024-49099
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2024-49099
- https://nvd.nist.gov/vuln/detail/CVE-2024-49098
- https://www.tenable.com/cve/CVE-2024-49098
- https://nvd.nist.gov/vuln/detail/CVE-2024-49094
- https://www.tenable.com/cve/CVE-2024-49094
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-49094
- https://nvd.nist.gov/vuln/detail/CVE-2024-49092
- https://www.tenable.com/cve/CVE-2024-49092
- https://nvd.nist.gov/vuln/detail/CVE-2024-49087
- https://www.tenable.com/cve/CVE-2024-49087
- https://nvd.nist.gov/vuln/detail/CVE-2024-49073
- https://www.tenable.com/cve/CVE-2024-49073
- https://nvd.nist.gov/vuln/detail/CVE-2024-49064
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-49064
- https://www.tenable.com/cve/CVE-2024-49064

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