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

CERT-MU Security Alert

Date of Issue: 18 October 2022

Windows Mark of the Web Bypass Zero-Day Vulnerability

Severity Level: High

Affected systems: Microsoft Windows

- Windows 10 v1803 and later
- Windows 7 with or without ESU
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2008 R2 with or without ESU

Description:

A zero-day vulnerability has been identified in the Windows Mark of the Web (MotW) security mechanism. The vulnerability can allow attackers to prevent Windows from applying (MotW) labels on files extracted from ZIP archives downloaded from the Internet. Windows automatically adds MotW flags to all documents and executables downloaded from untrusted sources, including files extracted from downloaded ZIP archives, using a special 'Zone.Id' alternate data stream. These MotW labels tell Windows, Microsoft Office, web browsers, and other apps that the file should be treated with suspicion and will cause warnings to be displayed to the user that opening the files could lead to dangerous behavior, such as malware being installed on the device.

Impact of the attack:

An attacker could deliver Word or Excel files in a downloaded ZIP that would not have their macros blocked due to the absence of the MotW (depending on Office macro security settings), or would escape the inspection by Smart App Control.

Since the zero-day was reported, it has been detected as exploited in attacks to deliver malicious files on victims' systems.

Workarounds

Microsoft has not released any patch yet.

Users are advised to take the following precautions:

- Be cautious when receiving emails with Zip attachments and do not open unknown emails with ZIP attachments.
- Scan attachments before opening them.
- Use an up-to-date anti-virus software
-

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
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