National Computer Board
Computer Emergency Response Team of Mauritius
(CERT-MU)

Targeted Alert

WinRAR Vulnerability puts millions of users worldwide at risk

Original Issue Date: October 07, 2015

Severity Rating: High

Affected Systems:

- All versions of WinRAR SFX

Description:

A new dangerous unpatched Zero-day Vulnerability has been detected in the latest version of WinRAR affecting over millions of users worldwide. WinRAR is one of the most popular utility program used to compress and decompress files with more than 500 Million installations worldwide. The vulnerability allows remote attackers to execute unauthorized system-specific code to take control of a target computer. The issue resides in the "Text and Icon" function of the "Text to display in SFX window" module. This vulnerability allows remote attackers to generate their own compressed archives with malicious payloads to cause execution of system specific code for compromise. The vulnerability requires an attacker to use social-engineering methods to trick a user into running a malicious executable file saved as a self-extracting archive (SFX) file on their computer.

Impact of the vulnerability

Exploitation of the vulnerability requires low user interaction (open file) without privilege system or restricted user accounts. Successful exploitation of the vulnerability in the WinRAR SFX software results in system, network or device compromise.

Workarounds:
No patch is currently available to fix this vulnerability. However, users are advised to:

- Use an alternate archiving software
- Do not click files received from unknown sources
- Use strict authentication methods to secure your system

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info: contact@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu