National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Mac vulnerability could provide persistent and stealthy access

Original Issue Date: June 05, 2015

Severity Rating: High

Affected Systems:

- Mac Mini 5.1
- MacBook Pro 9.2
- MacBook Pro Retina 10.1
- MacBook Pro 8.2
- MacBook Air 5.1
- Mac Pro 9.1

Description:

A critical vulnerability has been identified in Apple Mac Models and could be exploited by remote attackers to overwrite firmware and gain persistent root access to the computer. The vulnerability exists due to a flawed energy conservation implementation which left flash protections unlocked on the vulnerable Macs after they woke up from sleep mode. This enables an attacker to reflash the computer's firmware to install Extensible Firmware Interface (EFI) rootkit malware. The vulnerability is successfully exploited if used in conjunction with another exploit that provided root access. Once an attacker has root access, the only condition required for exploitation is that the computer enter sleep mode.

Impact:

This vulnerability is rated as critical since it can provide an attacker with persistent root access to a computer that may survive any disk wipe or operating system reinstallation.

Workarounds:

1. Users who are concerned about being targeted are advised to shut down their computers instead of using sleep mode, until a patch for the vulnerability is issued.

2. Affected Mac users are advised to keep their software up to date since this will prevent attacks using known exploits.

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