CERT-MU Weekly Security Bulletin

CERT-MU

CERT-MU Weekly Security Bulletin provides a summary of information security news, vulnerabilities, advisories and virus alerts for the week of July 10, 2017. This information is uploaded on CERT-MU website on a daily basis.

For more details, refer to CERT-MU website: http://cert-mu.org.mu.

THREAT ALERTS

Threat Alerts of the Week

Multiple Vulnerabilities in Microsoft Products

Multiple vulnerabilities have been identified in Microsoft Products, which can allow remote attackers to cause execution of arbitrary code, bypass security restrictions and gain knowledge of sensitive information on affected systems.

Read More

INFORMATION SECURITY NEWS

Hottest News

Magala Trojan Hijacks Internet Explorer, Then Commits Click Fraud

A click fraud Trojan called Magala is hijacking Internet Explorer browsers and opening virtual desktops on infected machines in order to artificially inflate various web pages' click counts. The Trojan which Kaspersky Lab researchers discovered and classified as potentially unwanted adware does not cause any significant harm to infected users, but it does cheat companies who pay for legitimate online ad services but instead are having their click stats boosted fraudulently by unscrupulous advertisers. Magala determines which version of Internet Explorer is running on an infected machine.

Read More

VULNERABILITIES

The table below shows the vulnerabilities related to various Operating Systems, Application software and Network devices discovered during the week of July 10, 2017. The vulnerabilities are organized according to their severity – High, Medium and Low. More details about the vulnerabilities and their countermeasures are available on the CERT-MU website.

VULNERABILITIES – HIGH			
Vendor / Product	**Vulnerability**	**Published Date**	**CERT-MU References**
Adobe	Adobe Flash Player Bugs Let Remote Users Obtain Potentially Sensitive Information and Execute Arbitrary Code	July 14, 2017	VN-2017-96
Adobe	Adobe Connect Input Validation Flaws Let Remote Users Conduct Clickjacking and Cross-Site Scripting Attacks	July 14, 2017	VN-2017-97

VULNERABILITIES – MEDIUM			
Vendor / Product	**Vulnerability**	**Published Date**	**CERT-MU References**
RSA	RSA Authentication Manager Input Validation Flaw Lets Remote Users Conduct Cross-Site Scripting Attacks	July 13, 2017	VN-2017-95
PHP	PHP Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information, Deny Service, and Execute Arbitrary Code	July 10, 2017	VN-2017-94

VIRUS ALERTS

The latest viruses and risks for this week are listed below. Users are required to follow the links on CERT-MU website for the removal instructions as proposed by the specific vendors.

Virus Alerts				
Name	**Type**	**Damage Level**	**Systems Affected**	**Release Date**
Trojan.Feratuser!bm	Trojan	Low	• Windows	July 13,2017
Trojan.Emotet	Trojan	Low	• Windows	July 13, 2017
Infostealer.Lockpos	Trojan	Low	• Windows	July 13, 2017
Ransom.Karo	Trojan	Low	• Windows	July 12, 2017
Backdoor.Dorshel	Trojan	Low	• Windows	July 12, 2017
Backdoor.Goodor	Trojan	Low	• Windows	July 12, 2017
Infostealer.Neupos	Trojan	Low	• Windows	July 11, 2017

Please note that the members who do not want to receive the weekly security bulletin, 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: http://cert-mu.org.mu