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 January 07, 2019. 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.

SECURITY ALERTS

Security Alerts of the Week

A Fake email was circulating on behalf of the Standard Chartered Bank, with the following details:

From: STANDARD CHARTERED BANK <comex.importadorabsas@yahoo.com>
Date: Tuesday, 8 January 2019 at 06:54
Subject: STANDARD CHARTERED BANK FOUND TRANSFER 8/01/2019

The email also contained an attachment: **PROVE OF PAYMENT.pdf.jar**

Read More

INFORMATION SECURITY NEWS

Hottest News

Microsoft Patches 7 Critical Vulnerabilities

Microsoft kicked off 2019 with a light Patch Tuesday listing 47 vulnerabilities with seven rated as critical. The seven critical issues all could lead to remote code execution and primarily impact Microsoft Edge, various versions of Windows 10 and Server and Chakra Core. The other overriding vulnerability, CVE-2018-8653, was patched by Microsoft in December, but industry analysts all reiterated the need for users to download the update.

Read More

VULNERABILITY NOTES

The table below shows the vulnerabilities related to various Operating Systems, Application software and Network devices discovered during the week of January 07,

2019. 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**
Cisco	Cisco Email Security Appliance Memory Corruption Denial of Service Vulnerability	January 10, 2019	**VN-2019-02**
Adobe	Adobe Reader DC JavaScript Read-Only Variables Arbitrary Overwrite Restrictions Bypass Vulnerability	January 09, 2019	**VN-2019-01**

VULNERABILITIES – MEDIUM			
Vendor / Product	**Vulnerability**	**Published Date**	**CERT-MU References**
Cisco	Cisco Webex Business Suite Cross-Site Scripting Vulnerability	January 11, 2019	**VN-2019-03**

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**
PUA.Superfluss	Potentially Unwanted APP	Low	• Windows	January 10, 2019

Hacktool.ProcHack!g1	Trojan	Low	• Windows	January 07, 2019
Hacktool.ProcHack	Trojan	Low	• Windows	January 07, 2019

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