UGANDA NATIONAL COMPUTER EMERGENCY RESPONSE TEAM (CERT.UG)

13|MAY|2017

INFORMATION SECURITY ALERT – IMPORTANT

Vulnerability Type: Ransomware

Severity: CERT.UG rates the severity of this vulnerability as **HIGH** due to ransomware's capability to cause data loss and negatively affect work environment productivity. This is Critical for all supported releases of **Microsoft Windows.**

Risk Assessment: Ransomware refers to sophisticated software that utilizes advanced encryption algorithms to block system files and demand payment in return for the key that can decrypt the blocked content. A ransomware attack is **VERY** damaging to an organization's data with very **HIGH** chances of complete data loss (on infected computers) as well as disruption in user productivity.

Vulnerability: This latest strain of ransomware attack vector is highly dangerous and evasive. To a large extent, we have noticed that the main attack vector is through exploiting the vulnerability in Server Message Block 1.0 (SMBv1). Exploitation of this vulnerability could allow a remote attacker to take control of an affected system. This is mainly noted for the following:-

a) Microsoft Windows Vista SP2
b) Windows Server 2008 SP2 y R2 SP1
c) Windows 7
d) Windows 8.1
e) Windows RT 8.1
f) Windows Server 2012 y R2
g) Windows 10
h) Windows Server 2016
i) Exchange and the IIS web server
j) Forefront Endpoint Protection, System Center Endpoint Protection, Security Essentials, Defender for Windows 7, 8.1, RT 8.1, 10 and Windows Server 2016

This attack is also made easier due to unpatched computers and lack of effective malware protection.

Risk Mitigation: It's important to note that chances of recovery of encrypted data are very **slim** especially with this latest strain of ransomware. The best mitigation strategy is prevention which can be achieved through the following:-

IMMEDIATE ACTION

a) Urgently apply the latest Microsoft Security Upate MS17-1010 – this reduces the affected SMB Server vulnerability used in this attack;
b) Aggressively update all firewall and AV signatures;
c) Keep up to date back-ups of all critical data;
d) Test and make a separate copy of the backup. A Copy of backed up data MUST be stored offline;
e) Test and practice data recovery procedures for effectiveness;
f) Ensure that all systems are patched up (especially all Microsoft installations, browsers and all its plugins);
g) Disable the execution of files with extension WNCR;
h) Disable macro scripts in files transmitted via email;
i) Scan all incoming and outgoing emails to detect threats and filter executable files (extensions such as exe and scr) from reaching end users;
j) Isolate communication to ports 137 and 138 UDP and ports 139 and 445 TCP in your organizations' network;

MUST DO:

k) Ensuring that the principle of 'Least Privilege Access' is adhered to for all users;
l) Ensuring effective use of effective anti-virus solutions on all computers as well as rootkit scanners on critical servers (effective anti-virus covers all the five distinct layers of protection: network, file, reputation, behavioral and repair). All e-mails and web downloads should be scanned to reduce exposure;
m) All web traffic should be filtered to block potential threats;
n) Review SMB Encryption as relates to your environment: https://technet.microsoft.com/en-us/library/dn551363(v=ws.11).aspx
o) Awareness and education on safe web surfing skills as well as e-mail usage to all staff on avoid spam and phishing campaigns (especially e-mails with the .zip or .scr attachments in e-mails from unknown sources).

Workaround: In the event that any user on your network has been compromised, kindly undertake the following:

a) Immediate disconnection the affected computer from the network. The more ransomware lingers on the network, the more it spreads;
b) Undertaking cleaning up any traces of ransomware;

c) Kindly inform us and we'll assist.

Note: Kindly contact us in case you would like us to:

a) Undertake an evaluation of your current network protection in order to identify improvement area; and
b) Hold an awareness session for all your staff members.

Uganda National Computer Emergency Response Team
Plot 7A, Rotary Avenue (Former Lugogo Bypass)
Twitter: @CERT.UG | Facebook: Cert1.ug
info@cert.ug
www.cert.ug