MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

FOR COMCEN/SIG USE

PRECEDENCE ACTION/PRECEDENCE INFO
"PRIORITY"

FM: CG, PA

TO: All Unit Commanders
Attn: G6/Signal Officer/IS Officer

INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA

INFO: CSAFP
Attn: J6

GROUP:
22 July 2016

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 2207-65-2016

1. References:

   a. Command Guidance, and;
   b. VAPT and PANET Monitoring Result.

2. As per above references, forwarded is the Cybersecurity Bulletin Number **063** with topic regarding **Removable Media and Unpatched or Outdated Software Vulnerabilities.**

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cybersecurity Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE	**PHONE NR:**
LTC JOEY T FONTIVEROS (INF) PA Chief, CMB, OG6, PA	6630
RELEASER'S NAME AND TITLE	
COL VENER ODILON D MARIANO GSC (SC) PA AC OF S FOR C4S, G6, PA	

Army Core Purpose: Serving the people. Securing the land.

HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMAND, CONTROL, COMMUNICATION, AND CYBER SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB

22 July 2016

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #63

Removable Media and Unpatched or Outdated Software Vulnerabilities.

Removable Media

The Threat

Removable media is any type of storage device that can be added to and removed from a computer while the system is running. Adversaries may use removable media to gain access to your system. Examples of removable media include:

- Thumb drives
- Flash drives
- CDs
- DVDs
- External hard drives

Indicators

The following is a list of suspicious indicators related to removable media. Adversaries and hackers may:

- Leave removable media, such as thumb drives, at locations for personnel to pick up
- Send removable media to personnel under the guise of a prize or free product trial

Effects include, but are not limited to:

- Corrupt files and destroyed or modified information
- Hacker access and sabotaged systems

Countermeasures

The following countermeasures can be taken to guard against removable media vulnerabilities.

Contractors: Follow your organization's removable media policy

DoD personnel:

- Do not use flash media unless operationally necessary and government-owned
- Do not use any personally owned/non-Government removable flash media on DoD systems
- Do not use Government removable flash media on non-DoD/personal systems
- Encrypt all data stored on removable media
- Encrypt in accordance with the data's classification or sensitivity level
- Use only removable media approved by your organization
- Store in GSA approved storage containers at the appropriate level of classification

Unpatched or Outdated Software Vulnerabilities

The Threat

Unpatched or outdated software provide vulnerabilities and opportunities for adversaries to access information systems.

Indicators

The following is a list of suspicious indicators related to unpatched and outdated software:

- Unauthorized system access attempts

- Unauthorized system access to or disclosure of information
- Unauthorized data storage or transmission
- Unauthorized hardware and software modifications

Effects include, but are not limited to:

- Corrupt files and destroyed or modified information
- Hard drive erasure and loss of information
- Hacker access and sabotaged systems

Countermeasures

The following countermeasures can be taken to guard against software vulnerabilities:

- Comply with the measures in your organization's policies, including the Technology Control Plan (TCP)
- Stay current with patches and updates
- Conduct frequent computer audits - Ideally: Daily
- At minimum: Weekly

- Do not rely on firewalls to protect against all attacks
- Report intrusion attempts
- Disconnect computer system temporarily in the event of a severe attack

Reference:

This was cross posted from:
http://cdsetrain.dtic.mil/cybersecurity/data/pdf/Common_Cyber_Threats_Indicators_and_Countermeasures.pdf

DO YOU WANT TO KNOW MORE? TALK TO US.

POCs:

a. **LTC JOEY T FONTIVEROS (INF) PA –** Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-6281057. Email: fontiverosjt@army.mil.ph.

b. **Sgt Mark Dave M Tacadena (SC) PA** – Branch NCO, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0998-5342877.