

CPF 0006-13-CID361-9H

6 February 2013



**Contact Information:**

**Cyber Criminal Intelligence Program**  
27130 Telegraph Road  
Quantico, Virginia 22134

**Phone: 571.305.4485**

**Fax: 571.305.4189**

**E-mail:**

**[cybercrimintel.cciu@us.army.mil](mailto:cybercrimintel.cciu@us.army.mil)**

**CCIU Web Page:**

**[www.cid.army.mil/cciu.html](http://www.cid.army.mil/cciu.html)**

**CID Cyber Lookout**  
On Point for the Army

**DISTRIBUTION:**

**This document is authorized for  
wide release with no restrictions.**



**"DO WHAT HAS TO BE DONE"**

## I DON'T WANT TO PLUG AND PLAY

### OVERVIEW:

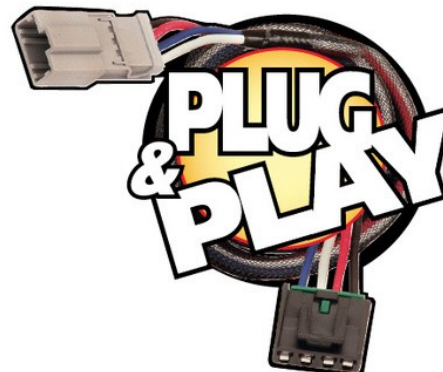
The purpose of this Cyber Crime Prevention Flyer (CCPF) is to inform all service members and Department of the Army civilians of a vulnerability involving [Universal Plug and Play](#) (UPnP), a feature found on virtually all home network routers, printers, servers, and other [network devices](#). CID elements are encouraged to brief supported installations and units on the contents of this CCPF.

### BACKGROUND:

Universal Plug and Play (UPnP) is a set of networking protocols that permits networked devices, such as a personal computer, printer, Internet gateway, Wi-Fi access point, smart phone, and other mobile devices to seamlessly discover each other's presence on the network and automatically establish functional network services for data sharing, communications, and entertainment. UPnP was designed primarily for residential networks.

Though this protocol at the surface seems harmless, it actually makes it extremely easy for hackers and other cybercriminals to discover and exploit these UPnP devices due to a recently discovered vulnerability. A research firm did a scan of the Internet and discovered over 50 million unique devices that could be remotely exploited by hackers as a result. Because these devices can be easily discovered by hackers, it makes them susceptible to attacks. If a hacker gains access to any UPnP device, it could allow them unfettered access to your network increasing your chances of becoming a victim of data loss, identity theft, or related crime.

Virtually every home in the United States uses some UPnP device, making them an easy target unless actions are taken to mitigate the risk.



## Safety Tips to Protect Your uPnP Devices:

- The U.S. Computer Emergency Response Team (US-CERT) recommends that home users disable UPnP (if possible) on all devices if it is not absolutely necessary. Check your owner manuals for instructions on how to disable the UPnP feature.
- Check your UPnP device's vendor for patches to ensure you have the most up to date firmware/software. These vendors include but are not limited to Cisco, D-Link, Linksys, Huawei Technologies, Sony, and many other vendors.

## Protecting Your Home Computer:

The U.S. Army Cyber Command offers free antivirus and firewall software for Department of the Army personnel to use on home computers: <https://www.acert.1stiocmd.army.mil/Antivirus/>

For more information about computer security and other computer related scams, we encourage readers to visit the [CCIU website](#) to review previous crime alert notices and crime prevention flyers.

## ADDITIONAL INFORMATION:

### U.S. Computer Emergency Response Team

- <http://www.kb.cert.org/vuls/id/357851>
- <http://www.kb.cert.org/vuls/id/922681>



### RAPID7

- <https://community.rapid7.com/community/infosec/blog/2013/01/29/security-flaws-in-universal-plug-and-play-unplug-dont-play>
- <https://community.rapid7.com/docs/DOC-2150>

### ZDNet

- <http://www.zdnet.com/homeland-security-disable-upnp-as-tens-of-millions-at-risk-7000010512/>

**Disclaimer:** The appearance of hyperlinks in this Cyber Crime Prevention Flyer (CCPF), along with the views and opinions of authors, products or services contained therein does not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations. Such links are provided consistent with the stated purpose of this CCPF.



**CCIU's "Toucan Lan" keeps an eye on cyber crime issues of interest to the Army community.**

**ICE**

**CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.**