Contact Information:
Cyber Criminal Intelligence Program
9805 Lowen Road, Building 193
Fort Belvoir, Virginia 22060-5598

Phone: 703.805.3499 (DSN 655)
Fax: 703.805.2351 (DSN 655)
E-mail:
cybercrimintel.cciu@us.army.mil

CCIU Web Page:
www.cid.army.mil/cciu.htm

2CAN 0008-10-CID361-9H 12 March 2010

ENERGIZER® BATTERY CHARGER SOFTWARE COULD LEAVE YOUR PC DRAINED

OVERVIEW:

The U.S. Computer Emergency Readiness Team (US-CERT) has reported a backdoor in the companion software for the Energizer DUO USB battery charger. This backdoor may allow an attacker to gain remote access and execute programs on an infected system. The software, which was discontinued by Energizer on March 5, 2010, was available for both Windows and Apple Mac OS X computer systems. Only the Windows version is affected by this vulnerability.

CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

IT JUST KEEPS ON GOING:

The Energizer DUO USB battery charger is a USB and AC charger for Nickel Metal Hydride (NiMH) batteries. Until recently, the manufacturer offered DUO users the ability to download optional software that allowed users to monitor the charging status of the batteries when the DUO was plugged into their PCs. While the hardware in and of itself is not known to cause any issues, the battery monitoring software installs a backdoor that allows unscrupulous persons to have remote access to the computer. This remote access can allow unauthorized person(s) to list directories, send and receive files, and execute programs. Although the manufacturer has removed the software from its website, the software is still believed to be in widespread use.

Consumers most likely were not expecting the Energizer software to carry a malicious tool. Normally, in operating systems such as Windows 7 or even Windows Vista, if you allow programs to access the internet you will normally receive a warning message. But since you got the software from a trusted source, chances are you'll skip past the warning and install it because you think you are only installing the battery monitor.

Symantec reported that it had conducted an analysis on a file received from the US-CERT. It was discovered that the file was a Trojan that opens a back door on a compromised computer and listens for commands on transmission control protocol (TCP) port 7777. "We were interested in finding out how long this file had been available to the public. The compile time for the file is May 10, 2007. It is impossible to say for sure that this Trojan has always been in this software, but from our initial inspection it appears so," explained Liam O. Murchu, Symantec's supervisor of security response operations for North America.

Energizer is working with US-CERT and government officials to understand how the malicious code was inserted into their software.

Remediation:

The US-CERT provides several solutions to remediate the vulnerabilities associated with this software. Refer to the details at the US-CERT website.

Protecting Your Home Computer:

The Army Computer Emergency Response Team offers free antivirus and firewall software for Department of the Army personnel to use on home computers. You must access the following link from a .mil computer system and authenticate with your CAC and PIN:

https://www.acert.1stiocmd.army.mil/Antivirus/

Additional Reporting and Information:

U.S. Computer Emergency Readiness Team
http://www.kb.cert.org/vuls/id/154421

Energizer Holdings, Inc.
http://phx.corporate-ir.net/phoenix.zhtml?c=124138&p=irol-newsArticle&ID=1399675&highlight=

ZDNet
http://blogs.zdnet.com/hardware/?p=7584

Symantec
http://www.symantec.com/connect/blogs/trojan-found-usb-battery-charger-software

The Security Blog
http://www.thesecurityblog.com/2010/03/usb-battery-chargers-with-malware/

Mitre Common Vulnerabilities and Exposures (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0103

ICE

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