Zero Day
Ryan Naraine and Dancho Danchev

March 8th, 2010

Energizer battery charger contains backdoor

Posted by Ryan Naraine @ 5:16 am

The United States Computer Emergency Response Team (US-CERT) has warned that the software included in the Energizer DUO USB battery charger contains a backdoor that allows unauthorized remote system access.

In an advisory, the US-CERT warned that he installer for the Energizer DUO software places the file UsbCharger.dll in the application's directory and Arucer.dll in the Windows system32 directory.

> When the Energizer UsbCharger software executes, it utilizes the UsbCharger.dll component for providing USB communication capabilities. UsbCharger.dll executes Arucer.dll via the Windows rundll32.exe mechanism, and it also configures Arucer.dll to execute automatically when Windows starts by creating an entry in the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run registry key.

US-CERT said that Arucer.dll is a backdoor that allows unauthorized remote system access via accepting connections on 7777/tcp.

Here's the major risk:

> An attacker is able to remotely control a system, including the ability to list directories, send and receive files, and execute programs. The backdoor operates with the privileges of the logged-on user.

Anti-malware researchers at Symantec have posed a detailed write-up of the Trojan discovery.

Energizer has issued a statement acknowledging the issue. The company said it has discontinued sale of this product and has removed the site to download the software. In addition, Energizer is directing consumers that downloaded the Windows version of the software to uninstall or otherwise remove the software from your computer.

REMOVE THE SOFTWARE:

According to US-CERT, the backdoor component of the Energizer UsbCharger software can be removed by deleting the Arucer.dll file from the Windows system32 directory. Because the backdoor hosted by rundll32.exe continues to run after the software has been uninstalled, the Windows may need to be restarted before this file can be removed.

Affected users should also block access to 7777/tcp. This helps to mitigate this vulnerability by preventing network connectivity to the backdoor.

> This may be achieved with network perimeter devices or host-based software firewalls. The Energizer UsbCharger software does not automatically add an exception to the Windows Firewall for 7777/tcp or the backdoor application. Therefore, the first time that Energizer UsbCharger is executed, the user will be prompted that “Run a DLL as an APP” has been blocked by the Windows Firewall.

Ryan Naraine is a journalist and security evangelist at Kaspersky Lab. He manages Threatpost.com, a security news portal. Here is Ryan's full profile and disclosure of his industry affiliations.

Email Ryan Naraine

For daily updates on Ryan's activities, follow him on Twitter.