Emergency Management and Response Information Sharing and Analysis Center

CIP BULLETIN 2-09 March 30, 2009

NOTE: *CIP Bulletins will be distributed as necessary to provide members of the Emergency Services Sector with timely, important, unclassified information potentially affecting the protection of their critical infrastructures. They are prepared by the Emergency Management and Response- Information Sharing and Analysis Center (EMR-ISAC) at (301) 447-1325 or by e-mail at emr-isac@dhs.gov.*

March 30, 2009 Contact: DHS Press Office, 202-282-8010

DHS RELEASES CONFICKER/DOWNADUP COMPUTER WORM DETECTION TOOL
Tool Allows Critical Partners to Assess Risks to Their Systems

WASHINGTON – The U.S. Department of Homeland Security (DHS) announced today the release of a DHS-developed detection tool that can be used by the federal government, commercial vendors, state and local governments, and critical infrastructure owners and operators to scan their networks for the Conficker/Downadup computer worm.

The department's United States Computer Emergency Readiness Team (US-CERT) developed the tool that assists mission-critical partners in detecting if their networks are infected. The tool has been made available to federal and state partners via the Government Forum of Incident Response and Security Teams (GFIRST) Portal, and to private sector partners through the IT and Communications sector Information Sharing and Analysis Centers (ISACs). Additional outreach to partners will continue in the coming days.

Department cyber experts briefed federal Chief Information Officers and Chief Information Security Officers today, as well as their equivalents in the private sector and state/local government via the ISACs and the National Infrastructure Protection Plan framework.

"While tools have existed for individual users, this is the only free tool – and the most comprehensive one – available for enterprises like federal and state government and private sector networks to determine the extent to which their systems are infected by this worm," said US-CERT Director Mischel Kwon. "Our experts at US-CERT are working around the clock to increase our capabilities to address the cyber risk to our nation's critical networks and systems, both from this threat and all others."

In addition to the development of this tool, DHS is working closely with private sector and government partners to minimize any impact from the Conficker/Downadup computer worm. This worm can infect Microsoft Windows systems from thumb drives, network share drives, or directly across a corporate network if network servers are not protected by Microsoft's MS08-067 patch.

US-CERT recommends that Windows Operating Systems users apply Microsoft security patch MS08-067 (http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx) as quickly as possible to help protect themselves from the worm. This security patch, released in October 2008, is designed to protect against a vulnerability that, if exploited, could enable an attacker to remotely take control of an infected system and install additional malicious software.

Home users can apply a simple test for the presence of a Conficker/Downadup infection on their home computers. The presence of an infection may be detected if users are unable to connect to their security solution Web site or if they are unable to download free detection/removal tools.

If an infection is suspected, the system or computer should be removed from the network. In the case of home users, the computer should be unplugged from the Internet.

Instructions, support and more information on how to manually remove a Conficker/Downadup infection from a system have been published by major security vendors. Each of these vendors offers free tools that can verify the presence of a Conficker/Downadup infection and remove the worm:

Symantec:
http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-011316-0247-99.

Microsoft:
http://support.microsoft.com/kb/962007.
http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx.
Home users may also call Microsoft PC Safety hotline at 1-866-PCSAFETY, for assistance.

McAfee:
http://www.mcafee.com/us/threat_center/default.asp.

US-CERT encourages users to prevent a Conficker/Downadup infection by ensuring all systems have the MS08-067 patch, disabling AutoRun functionality (see http://www.us-cert.gov/cas/techalerts/TA09-020A.html), and maintaining up-to-date anti-virus software.

In addition, US-CERT recommends that computer users and administrators implement the following preparedness measures to protect themselves against this vulnerability, and also from future vulnerabilities:

• Keep up-to-date on security patches and fixes for your operating system. The easiest way to do this is to set your system to receive automatic updates, which will ensure you automatically receive security updates issued by Microsoft. If your system does not allow automatic updates, we recommend that you manually install the Microsoft security patch today through Microsoft Update at http://update.microsoft.com/microsoftupdate.

- Install anti-virus and anti-spyware software and keep them up-to-date.
- Enable a firewall which will help block attacks before they can get into your computer.

To access the alerts for this vulnerability and for additional information on cyber security tips and practices, please visit www.us-cert.gov.