

DAS Enterprise Security Office Advisory

Network Printers

February 13, 2009

Hewlett Packard recently released a new security patch to fix an authentication bypass vulnerability in specific network printers. The Enterprise Security Office is using this opportunity to remind agencies of the importance of securing network printers in general. Network printers are frequently overlooked when securing office networks; sometimes left with default configurations and not patched, they represent a risk to the office network environment.

Network based printers are much more than just a print device. They typically have full operating systems, hard drives, and a full complement of communication services. Built-in services such as ftp, tftp, e-mail, web server, and snmp are increasingly the target of choice for hackers wanting to remain undetected and to gain a foothold in the office network. Because network printer devices are frequently left unsecured with default passwords and utilizing factory default settings they are easy targets.

Example attacks against printers include bridging between networks (i.e wireless to LAN or vice-versa), sniffing network traffic to steal sensitive data, redirection and spoofing of network traffic, malware distribution and email spam generation.

Applicable Devices:

All network printing devices, multifunction copiers, and network based fax machines.

Recommendations:

The following are some basic recommendations for printer security in all environments.

- Keep printers up-to-date with latest firmware releases
- Change the default passwords and settings
- Turn off unnecessary services and features
- Consider requiring authentication to print and to use other services (particularly with multifunction devices)
- If available, encrypt the printer's hard disk
- Include printers in periodic vulnerability assessments of office networks
- Use appropriate network segmentation, ensuring that printers are separated from networks with critical services
- Use printer accounting features and review logs regularly
- Dispose of printers in accordance with the statewide "Sustainable Acquisition and Disposal of Electronic Equipment Policy" to ensure sanitization of the hard disk before release

References:

- It's Not Exciting, but Neglecting Printer Security is Dangerous:
 - <http://www.itbusinessedge.com/cm/blogs/weinschenk/its-not-exciting-but-neglecting-printer-security-is-dangerous/?cs=13617>
- Certain HP LaserJet Printers, HP Color LaserJet Printers, and HP Digital Senders, Remote Unauthorized Access to Files:
 - <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01623905>
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4419>
- Highlighting Printer Security Issues:
 - <http://www.itworld.com/071101networking>
- Sustainable Acquisition and Disposal of Electronic Equipment Policy:
 - <http://oregon.gov/DAS/OP/docs/policy/state/107-009-0050.pdf>