MULTIFUNCTION PRINTER VULNERABILITIES

EXECUTIVE SUMMARY

(U) The purpose of this bulletin is to explore potential vulnerabilities of multifunction printers (MFPs) and provide current mitigation strategies to the CIKR community at large. Specifically, the possibility of using MFPs, a common and overlooked enterprise device, for network intrusion and malicious activity is explored.

(U) This bulletin will draw primarily from several recent examples of demonstrated vulnerabilities by cyber researchers. Notably, a recent demonstration by a university researcher exploiting a firmware vulnerability in a major printer manufacturer is examined. Also, at a December technology conference, the Chaos Communication Congress, two separate lectures were presented on multifunction printer vulnerabilities. The lectures illustrated how a common enterprise device, the office printer, can be exploited to serve as a point of entry into a network and function in a manner very similar to that of a workstation compromised by malicious software.

BACKGROUND

(U) In December of 2011, the 28th Chaos Communication Congress (28C3), a four day technology conference, was held in Berlin. The 28C3 conference consisted of lectures and workshops. Included in the lectures were two presentations on networked, multifunction printers. One lecture focused on a Hewlett-Packard (HP) printer vulnerability and the other on an Adobe PostScript vulnerability.

(U) On December 29th, Ang Cui and Jonathan Voris demonstrated a vulnerability in HP printers with their lecture, “Print Me If You Dare: Firmware Modification Attacks and the Rise of Printer Malware.” At the time of the presentation, the team presented their findings that certain HP printers contain a vulnerability that allows an unsigned (and possibly malicious) remote firmware update to be executed on a HP printer. The research team was able to successfully design malware with capabilities that include port scanning, using the MFP as a proxy for network exploration, and exfiltrating data from print-jobs. According to the research team, this malware could be pushed to the printer either by directly connecting to port 9100 or by embedding their malicious firmware in a document and having the user print the document.

(U) According to Cui’s research1, this vulnerability was disclosed on November 21, 2011. On December 23, 2011, HP released new code signing firmware for the affected printers. This vulnerability disclosure generated attention in the press, including the erroneous claim that HP printers were catching fire. HP

issued a statement on November 29, 2011, stating that the “thermal breaker” contained in their printers would prevent a fire. Cui’s research also prompted a January 3, 2012, statement by Xerox regarding their MFP security. Xerox instructed customers with applicable products to password protect their firmware update feature.

(U) Receiving less press than the lecture on the HP vulnerability, Andrei Costin2 presented his research on printer exploitation one day previous to the presentation dealing with the HP vulnerability. Costin’s presentation, “Hacking MFPs, Part 2 – PostScript: Um, you’ve been hacked,” focused on an Adobe PostScript vulnerability in printers. Costin, who has been presenting on printer hacking since 2010, proposed using malicious PostScript and social engineering in order to infiltrate a network. An example presented by Costin was sending an individual on the targeted network a coupon that contained the malicious PostScript, when printed the intruder would be able to exfiltrate data from the MFP.

(U) Another third party trusted industry partner examined HP and Xerox printers and confirmed that printers from both manufacturers are susceptible to remote firmware update vulnerabilities.

(U) As demonstrated by the speakers, both the HP firmware and PostScript methods of attack can be conducted in a lab setting. The PostScript vulnerability appeared to lack some features found in the HP vulnerability, such as functioning as a port scanner. Judging by the presentation, the HP vulnerability does require more specific targeting, such as knowing what MFP is used by the target so that a compatible firmware can be crafted. On the other hand, the PostScript exploit was much more neutral with respect to its compatibility to targets. While the PostScript demonstration was done with Xerox products, it did not appear that any particular manufacturer or model was required—just a MFP that will readily process PostScript documents.

(U) Both lectures explained that their exploits could be accomplished remotely, through the use of social engineering and a document injected with malware. Additionally, both lectures took time to point out the large number of Internet-facing MFPs they discovered. According to Cui’s research, over 75,000 HP printers are on the Internet and readily available. Cui identified 43 printers belonging to government and nine printers named “payroll”—all nine belonging to educational institutions.

(U) Focusing on MFPs as a target, regardless of their manufacture, is appealing because they are not the traditional target of servers or workstations. Despite their hardware, many individuals do not see MFPs as “computers”. This mentality can lead to a lack of concern when it comes to security and MFPs. While there are plenty of products available for scanning, detecting, analyzing, and cleaning traditional targets, the common MFP has slipped by as an area of concern. As pointed out in the 28C3 lectures, this lack of concern for MFP security makes them an excellent device to target, infect, and utilize as a staging point for network exploitation and data exfiltration.

(U) It should be noted that researching printer vulnerabilities is not a new topic. Material is readily available dating back more than a decade on printer vulnerabilities. For example, HP’s JetDirect hardware has previously been the focus of research. What is different from previous research, particularly with respect to Cui’s work, is the focus on created malicious firmware to “own” a MFP.

(U) Essentially, Cui’s research supports the case that MFPs require greater examination in relation to security. A printer is no longer “just a printer”. MFPs deserve a greater level of concern because they can be exploited in the same manner as a workstation.

---

(U) The HP vulnerability required that the MFP be able to accept remote firmware updates and not require signed firmware. Once these conditions are met, Cui described two attacks methods: First, an active attack, in this case the attack directly connects to the printer on port 9100. After establishing a connection with the MFP, the malicious firmware can be updated to the printer. If the target has not implemented measures to limit access to the MFP (e.g. a password) and left it exposed to the Internet, this method is fairly straightforward. As previously mentioned, Cui was able to find a large number of MFPs exposed to the Internet. The second method of attack is taking the malicious firmware and injecting it into a document. Once the user prints this tainted document—possibly through the use of social engineering—the MFP will be updated with the malicious firmware. This method would take more skill on the part of the attacker, but would allow an attacker to gain access to a greater number of printers, more than just those exposed to the Internet. Cui showed that this method would allow access to MFPs behind an organization’s firewall, MFPs thought to be hidden and secured from the Internet.

(U) The methods outlined by Cui would require crafting a custom firmware compatible with the targeted MFP. Cui stated that he would release a tool, HPacker, for examining and crafting custom firmware for the vulnerability he discovered.

(U) Costin’s PostScript method of attack was similar to Cui’s, either gain access to a MFP exposed to the Internet or have a user print a document with tainted PostScript. Once this document is processed by the printer, the attacker has control of the MFP.

MITIGATION


(U) While the HP code signing firmware was not released before Cui’s lecture, many of his major mitigation steps are still worthwhile even with the latest firmware release, such as disabling remote firmware updates, using access control lists and passwords, and isolating printers from sensitive networks. Note that Cui does not state the code signing firmware is a secure solution, but that disabling remote firmware updates is a secure solution. This is important considering how the HP Security Bulletin shows that all models listed can disable remote firmware updates, but not all models can utilize code signing firmware.

(U) Similar to Cui, Costin also presented his ideas on protecting MFPs. One major suggestion by Costin, whose lecture used Xerox MFPs, was the disabling Language Operator Authorization in order to prevent systems modifications. Costin suggested other solutions, such as sandboxing printers in the network.

(U) As mentioned above, Xerox recently alerted customers to use the password protect option for firmware updates on products susceptible to this style of exploit.

POUNTS OF CONTACT

(U) Please direct all questions to the NCCIC Duty Officer (NDO). NCCIC will continue to coordinate with the appropriate component organizations listed below:

<table>
<thead>
<tr>
<th>NCCIC Duty Officer</th>
<th>US-CERT</th>
<th>NCS/NCC</th>
<th>ICS-CERT</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:NCCIC@HQ.dhs.gov">NCCIC@HQ.dhs.gov</a></td>
<td><a href="mailto:SOC@US-CERT.gov">SOC@US-CERT.gov</a></td>
<td><a href="mailto:NCS@HQ.dhs.gov">NCS@HQ.dhs.gov</a></td>
<td><a href="mailto:ICS-CERT-SOC@dhs.gov">ICS-CERT-SOC@dhs.gov</a></td>
</tr>
<tr>
<td>(703) 235-8831</td>
<td>(888) 282-0870</td>
<td>(703) 235-5080</td>
<td>(877) 776-7585</td>
</tr>
</tbody>
</table>