Samsung to issue updates in response to printer alert

November 29 2012, by Nancy Owano

(Phys.org)—Samsung has issued a response to CERT's vulnerability advisory about Samsung networked printers but the response may have left printer owners wondering what to do next. Samsung said that it is aware of and has resolved the security issue affecting Samsung network printers and multifunction devices. "The issue affects devices only when SNMP is enabled, and is resolved by disabling SNMP." The company offered the reminder that it takes all matters of security seriously. They said that were they not aware of any customers affected by this vulnerability. Samsung said that it intends to release updated firmware for all current models by November 30, and all other models will receive an update by the end of the year.

Nonetheless, it added, any customers concerned about the vulnerability can disable SNMPv1.2 or use the secure SNMPv3 mode until the firmware updates are made.

Samsung's SNMP advice, however, appeared to generate more questions than answers, motivating at least one news service, CNET, to contact Samsung in order to clarify the issue.

That is because the U.S. Computer Emergency Response Team (CERT) Vulnerability Note (VU#281284), issued first on November 26 and then revised on Wednesday said that a hardcoded Simple Network Management Protocol (SNMP) full read-write community string remains active even when SNMP is disabled in the printer management utility. The account in the firmware will still allow access to the device even if management functions are disabled in the printer's software utility.

The CERT warning spoke about a Samsung printer firmware backdoor administrator account. This is a hardcoded account in the printers that could allow a remote attacker to take control of an affected device. The note pertained to Samsung printers as well as some Dell printers manufactured by Samsung. "A remote, unauthenticated attacker could access an affected device with administrative privileges," US-CERT said. "Secondary impacts include: the ability to make changes to the device configuration, access to sensitive information (e.g., device and network information, credentials, and information passed to the printer), and the ability to leverage further attacks through arbitrary code execution."

CERT then referenced that the "reporter has stated that blocking the custom SNMP trap port of 1118/udp will help mitigate the risks."

Samsung and Dell have stated that any models released after October 31 if this year are not affected by this vulnerability.

The CERT note was a result of findings by Neil Smith, a security researcher, who then contacted US-CERT on November 26, telling them that Samsung printer firmware contains a hardcoded backdoor administrator account that could allow remote network access exploitation and device control.

More information: www.kb.cert.org/vuls/id/281284

Citation: Samsung to issue updates in response to printer alert (2012, November 29) retrieved 10 April 2024 from https://phys.org/news/2012-11-samsung-issue-response-printer.html