Palo Alto Networks Provides Enterprise Customers Protection from Heartbleed Vulnerability

April 11, 2014

SANTA CLARA, Calif., April 11, 2014 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the leader in enterprise security, announced it provides protection from the Heartbleed bug (vulnerability CVE-2014-0160) for its enterprise customers.

According to the US Cert Alert (TA14-098A) that was documented on April 8, 2014, this vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the heartbeat extension.

QUOTES

- "We had a lot of people worried when they saw the alert on the Heartbleed vulnerability; I just sat back and smiled because I had seen that we were already protected with our Palo Alto Networks security platform."
    - Neal Moss, systems and network analyst, IT infrastructure at BYU Hawaii
- "The breadth of risk for Heartbleed goes beyond web applications like Yahoo!, Google and Facebook. Getting a good handle on all the vulnerable services that make up an organization's attack surface can be a daunting challenge. There is hope though, because Palo Alto Networks is in a unique position to protect against Heartbleed through the next-generation design of our enterprise security platform, and the automated protections we released, preventing exploitation of this vulnerability for our customers."
    - Raj Shah, senior director of cybersecurity at Palo Alto Networks

For its customers, Palo Alto Networks provides unique protection from exploitation of the Heartbleed vulnerability, including:

- **Innovative approach to identifying threats** – unlike other security products, our platform natively decodes all traffic at the application layer, regardless of port and the protocol used, including SSL/TLS tunnels. Therefore, we are able to decompose the protocol (SSL in this case) to detect anomalies in ways that cannot be done with legacy network security devices.
- **Automated vulnerability protection** – Multiple content updates were automatically sent to our customers starting April 9th, 2014. These vulnerability protections detect and immediately block attempted exploitation of the vulnerability (content updates 429 and 430, which include IPS vulnerability signature IDs 36416, 36417, 36418, and 40039).
- **Inherent PAN-OS features** – our core operating system [PAN-OS], is not impacted by CVE-2014-0160 because it does not use a vulnerable version of the OpenSSL library.

For enterprises who are not Palo Alto Networks customers that are concerned about protecting themselves, we suggest, at a minimum, updating web servers to the latest patched version of OpenSSL available as of April 7, 2014 (1.0.1g), and immediately replacing SSL private keys after the patch is in place.

More about the vulnerability

The Heartbleed bug is associated with a critical vulnerability in OpenSSL that was recently disclosed that affects servers running OpenSSL 1.0.1 through 1.0.1f, estimated at "over 17% of SSL web servers which use certificates issued by trusted certificate authorities." At worst, the vulnerability can lead to compromise of nearly the total contents of any server running affected versions of OpenSSL-enabled application, including internal services.

To learn more about Palo Alto Networks protection from Heartbleed, visit: http://researchcenter.paloaltonetworks.com/2014/04/real-world-impact-heartbleed-cve-2014-0160-web-just-start/

About Palo Alto Networks

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection based on what matters most in today's dynamic computing environments: applications, users, and content. Find out more at www.paloaltonetworks.com.

Logo - http://photos.prnewswire.com/prnh/20130508/SF04701LOGO

SOURCE Palo Alto Networks

Jennifer Jasper-Smith, Head of Corporate Communications, 408-638-3280, jjsmith@paloaltonetworks.com; or Tim Whitman, Voce Communications, 617-721-5994, twhitman@vocecomm.com