F5 Helping Customers Mitigate Heartbleed Bug

Apr 11, 2014 5:34 PM

Little or no immediate action required for most customers

SEATTLE--(BUSINESS WIRE)-- In response to widespread concern about this week's OpenSSL Heartbleed bug and related attacks, F5 Networks today issued a statement and some simple guidance for its customers.

Companies using F5® BIG-IP® Local Traffic Manager™ (LTM®) to terminate SSL connections already have the necessary protections in place to secure their applications against the Heartbleed bug. For companies terminating SSL connections on application servers (not utilizing F5 SSL offload), the threat can be immediately mitigated through open, extensible F5 iRules®. Customers are encouraged to visit F5's DevCentral™ and f5.com for more information.

"For organizations using F5 BIG-IP Local Traffic Manager (LTM) with our SSL stack, applications are already protected from the Heartbleed vulnerability," said Mark Vondemkamp, VP of Product Management, Security at F5. "They have been protected from the Heartbleed bug since it was introduced in OpenSSL."

For those not using F5 for SSL offload, the company offers a unique and effective approach to protect against severe, industry-wide vulnerabilities like Heartbleed. Using extensible iRules from F5, customers can easily eliminate the possibility that attacks seeking to exploit the Heartbleed vulnerability will reach back-end servers, providing protection while sever certificates are being updated.

Details

The Heartbleed bug exploits a vulnerability in the OpenSSL library, enabling hackers to steal sensitive information typically protected by TLS encryption, which is the standard for securing Internet communications such as email, instant messaging, and VPNs, as well as applications. The Heartbleed bug can enable hackers to peer into and steal sensitive corporate, government, and personal data, putting intellectual property, state secrets, and personally identifiable information (PII) at risk. It also allows attackers to lift typically private user names, sessions, and passwords, thereby enabling them to imitate users and services, making an array of services and information open and vulnerable to attack and theft.

The F5 platform allows for a unique and effective approach to protect against a severe, industry-wide bug like Heartbleed.

"F5's full-proxy architecture enables protection against zero-day threats and vulnerabilities," added Vondemkamp. "This is an industry-tested, high-performance solution that delivers exceptional security, even for severe threats such as the Heartbleed bug."

About F5

F5 (NASDAQ: FFIV) provides solutions for an application world. F5 helps organizations seamlessly scale cloud, data center, and software defined networking (SDN) deployments to successfully deliver applications to anyone, anywhere, at any time. F5 solutions broaden the reach of IT through an open, extensible framework and a rich partner ecosystem of leading technology and data center orchestration vendors. This approach lets customers pursue the infrastructure model that best fits their needs over time. The world's largest businesses, service providers, government entities, and consumer brands rely on F5 to stay ahead of cloud, security, and mobility trends. For more information, go to f5.com.

You can also follow @f5networks on Twitter or visit us on Facebook for more information about F5, its partners, and technologies.

F5, BIG-IP, Local Traffic Manager, LTM, iRules, and DevCentral are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries. All other product and company names herein may be trademarks of their respective owners.

This press release may contain forward-looking statements relating to future events or future financial performance that involve risks and uncertainties. Such statements can be identified by terminology such as "may," "will," "should," "expects," "plans," "anticipates," "believes," "estimates," "predicts," "potential," or "continue," or the negative of such terms or comparable terms. These statements are only predictions and actual results could differ materially from those anticipated in these statements based upon a number of factors including those identified in the company's filings with the SEC.

☐

F5 Networks, Inc.
Alane Moran, 206-272-6850
a.moran@f5.com
or
Waggener Edstrom Worldwide
Gordie Hanrahan, 425-638-7048
ghanrahan@waggeneredstrom.com

Source: F5 Networks, Inc.