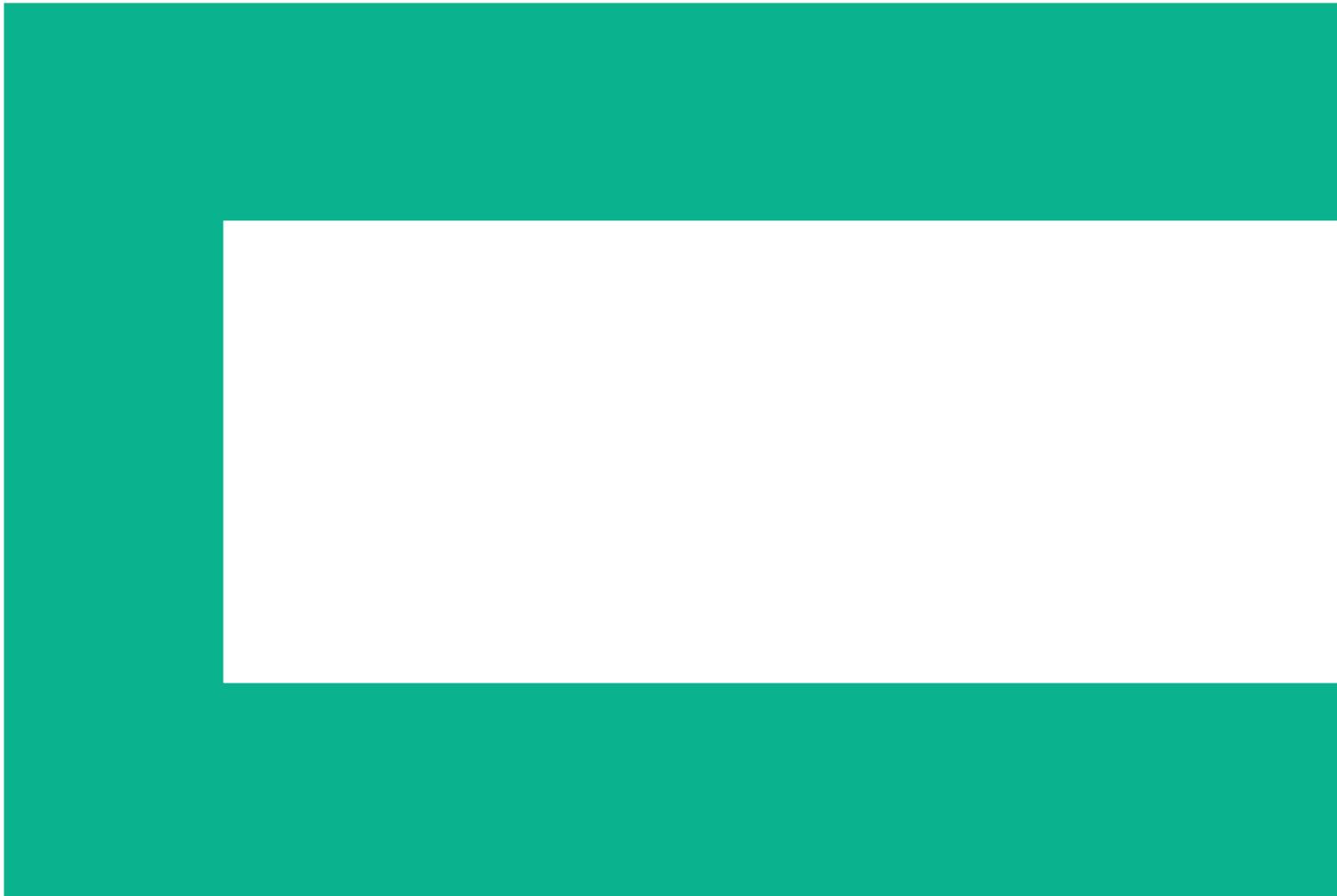




Combat top security vulnerabilities

HPE TippingPoint intrusion prevention system



The year 2014 marked a new pinnacle for hackers. Vulnerabilities were uncovered in some of the most widely deployed software in the world—some of it in systems actually intended to make you more secure. HPE TippingPoint next-generation intrusion prevention system (IPS) and next-generation firewall (NGFW) customers rely on us to keep their networks safe. And when it comes to cyber threats, every second matters. So how did HPE TippingPoint do? This brief highlights the top security vulnerabilities of 2014—the ones that sent corporate security executives scrambling to protect their businesses. And it describes how HPE TippingPoint responded to keep our customers safe.

Heartbleed—HPE TippingPoint intrusion prevention system stops blood flow early

Any vulnerability is concerning, but when a vulnerability is discovered in software designed to assure security, it leaves businesses exposed and vulnerable. That was the case with the Heartbleed vulnerability disclosed by the OpenSSL project on April 7, 2014. They found the vulnerability in versions of OpenSSL—the open-source cryptographic library widely used to encrypt Internet traffic.

Heartbleed grew from a coding error that allowed remote attackers to read information from process memory by sending heartbeat packets that trigger a buffer over-read. As a demonstration of the vulnerability, the OpenSSL Project created a sample exploit that successfully stole private cryptography keys, user names and passwords, instant messages, emails, and business-critical documents and communications.

We responded within hours to protect TippingPoint customers. On April 8, we released a custom filter package to defend against the vulnerability. This temporary solution stopped the blood flow for our customers, and we released the official HPE TippingPoint Digital Vaccine on April 10 providing a comprehensive vulnerability and intrusion prevention system for Heartbleed. Weeks later, HPE Security Research found a zero-day vulnerability in the same author's piece of OpenSSL code. HPE TippingPoint protected our customers more than 43 days in advance of OpenSSL patching the vulnerability.

ShellShock—TippingPoint bashes Bash bug

While Heartbleed allowed hackers to steal data from memory, ShellShock allowed them to actually take control of a computer and execute commands just as a local administrator might. This is due to a vulnerability in the GNU Bourne Again Shell (Bash), a command interpreter implemented in MacOS and all mainstream versions of Linux®. It gives remote attackers the ability to embed commands in HTTP requests that are then executed by the target system. The vulnerability was disclosed on September 24, 2014. And on September 25, Wired reported that hackers were already exploiting the bug in thousands of machines to launch botnet distributed denial-of-service (DDoS) attacks.¹

Fortunately, HPE TippingPoint intrusion prevention system also moved quickly. On the same day as the disclosure, we released a custom filter package to our customers to block attacks exploiting the vulnerability and notify security teams of the attempted exploit. And within two days, we released HPE TippingPoint Digital Vaccine to provide comprehensive network security protection from these vulnerabilities.

POODLE—TippingPoint ahead of the pack

POODLE stands for “Padding Oracle on Downgraded Legacy Encryption”—an innocuous name for a potentially damaging vulnerability. It’s a fault in version 3 of the Secure Sockets Layer protocol (SSLv3) used to encrypt traffic between a browser and a website or between a user’s email client and mail server. When used in a man-in-the-middle attack, POODLE allows an attacker to extract the plaintext in parts of an SSL connection, usually cookie data. That could allow the attacker to hijack and decrypt the session cookie that identifies a user to a service like Twitter or Google™ and take over the account without needing the user’s password.

Google security researchers disclosed POODLE October 14, 2014. Although SSL 3.0 is nearly 15 years old, support for it remains widespread because nearly all browsers support it, and browsers will often retry failed connections with older protocol versions including SSL 3.0.

In this case, HPE TippingPoint next-generation intrusion prevention system was ahead of the pack. Investigation at HPE DV Labs determined that TippingPoint customers were already able to detect SSLv3 negotiations through an existing Digital Vaccine filter that we distributed on May 6, 2014—161 days before the vulnerability was disclosed. The filter was originally distributed in disabled mode, so TippingPoint customers had only to change the deployment mode to activate it. Because the filter would detect any attempt to use SSLv3, we also advised our customers how to baseline their traffic before enabling the filter to avoid unexpected business impact. As a smart best practice, you should always know what applications are being used and sent in your network. Blocking unknown applications is one way to prevent attacks from POODLE-like vulnerabilities in the future.

¹ Andy Greenberg, Hackers Are Already Using the Shellshock Bug to Launch Botnet Attacks, Wired, September 25, 2014.

How HPE TippingPoint stops threats

HPE TippingPoint next-generation intrusion prevention system (NGIPS) and next-generation firewall (NGFW) are powered by security intelligence from HPE Security Research and HPE TippingPoint Digital Vaccine Labs (DVLabs). In addition to the Hewlett Packard Enterprise internal security research team, our Zero-Day Initiative pays independent researchers to find and report vulnerabilities.

When we identify a vulnerability or receive a disclosure from another source, we create a vulnerability filter. These filters don't just identify and block known exploits; they are "virtual patches" that can detect any attempt to exploit the vulnerability. So hackers cannot escape detection just by modifying the exploit. There are currently more than 8,200 vulnerability filters available to HPE TippingPoint customers right out of the box, and we push new filters to TippingPoint customers weekly. In fact, we have released more than one filter per day for the past 12 months.

More than 3,000 researchers are working to keep HPE TippingPoint customers updated with the latest security protection from known and unknown threats. As a result, we have received the Frost & Sullivan Market Share Leadership Award for Vulnerability Research four years in a row.



Conclusion

When it comes to threats, every second matters. That's why HPE TippingPoint intrusion prevention system acts quickly to block them before they can damage your business. We discover and protect you from vulnerabilities in the software you use—sometimes even before hackers can exploit them. And we protected our customers from the biggest threats of 2014 on day one. Learn how we can protect your business at: hpe.com/go/TippingPoint.

HPE TIPPINGPOINT—PROTECTION ON DAY ONE

Vulnerability	Severity ²	Date disclosed	HPE TippingPoint protection available
Heartbleed	Medium	4/7/2014	Day 1
ShellShock	High	9/24/2014	Day 1
POODLE	Medium	10/14/2014	Day 1

² Severity as reported in the NIST National Vulnerability Database.



Sign up for updates

★ Rate this document



Learn more at hpe.com/go/software

© Copyright 2015 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

© 2012 Google Inc. All rights reserved. Google and the Google Logo are registered trademarks of Google Inc. Oracle are registered trademarks of Oracle and/or its affiliates. Red Hat® Enterprise Linux Certified is a registered trademark of Red Hat, Inc. in the United States and other countries. Red Hat® Enterprise Linux Certified are trademarks of Red Hat, Inc. in the United States and other countries.

4AA5-6440ENN, November 2015, Rev. 1