Revised September 29th, 2014 FireEye Security Notice

Statement About "Shellshock" Vulnerability: CVE 2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, and CVE-2014-6278

Summary

On September 24th, 2014 a publicly disclosed vulnerability was revealed in the UNIX/Linux tool, Bash (Bourne-Again Shell), a widely used software utility. In the following days, additional vulnerabilities in the same area were discovered. The set of vulnerabilities, collectively known as Shellshock, are a serious issue for many organizations and may allow arbitrary remote code execution on vulnerable systems using Bash. The CVE numbers that are part of this are CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, and CVE-2014-6278. Links with details for each of these are below:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7186

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7187

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6277

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6278 (expected location)

What Is The Impact To FireEye Products and Services?

FireEye continues to evaluate Shellshock's impact to all products and services within our portfolio. **FireEye has additional details and updates available for customers that will be provided directly through customer support channels.** FireEye will continue to update this notice periodically as more information becomes available. This will include updates on specific products, dates for remediation if required, and mitigating actions if necessary. If no patch is currently available, FireEye leverages best-practice compensating controls such as Web Application Firewalls, FireEye NX with IPS, FireEye Threat Analytics Platform (TAP), and others. This helps us detect and mitigate threats to our products and services that might otherwise be susceptible to these unpatched vulnerabilities.

Best Practices

FireEye recommends that customers implement the following best practices when possible. These will help protect customers between the times when new vulnerabilities are discovered, and customers are able to update.

- Always keep the product version up-to-date.
- Limit network access to the management interface(s) of the appliance with firewalls or similar measures.
- Only issue accounts to trusted administrators.
- Utilize strong passwords.
- Restrict physical access to the appliance to trusted administrators.
- **Specifically for Shellshock:** Use static addressing instead of DHCP for FireEye appliances.

Notes

This advisory will be updated as patch status changes, or as other information becomes available.

Revision history:

- September 25th, 2014 – Initial version
- September 26th, 2014 – Update 1 (added details to Impact to FireEye)
- September 29th, 2014 – Update 2 (added new vulnerabilities in Summary)

For further information contact FireEye Customer Support.

http://www.fireeye.com/support/contact-customer-support.html

To report vulnerabilities in FireEye products, please email Security[at]FireEye.com or visit http://www.fireeye.com/security.