Revised October 16, 2014 FireEye Security Notice

Statement About "POODLE"/SSL 3.0 Vulnerability: CVE 2014-3566

Summary

On October 14, 2014, a publicly disclosed vulnerability was revealed in SSL version 3.0, which allows the plain text of secure connections to be calculated by a network attacker. The POODLE vulnerability targets client systems. If the system is vulnerable, an attacker must compromise a communications channel, such as an open Wi-Fi connection, to successfully execute a Man-in-the-Middle attack. CVE-2014-3566 has been assigned for this vulnerability; details can be found at the below link:

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566

What Is The Impact To FireEye Products and Services?

FireEye is in the process of evaluating POODLE'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). As always, FireEye recommends following the below general best practices to limit exposure in the case of a vulnerability such as POODLE.

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.

- Reconfigure clients to not support SSL v3.0.
- 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.

Notes

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

Revision history:

- October 15, 2014 – Initial version
- October 16, 2014 – Updated Best Practices

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.