Image not found
https://it.ucsf.edu/sites/it.ucsf.edu/themes/custom/it_new/logo.png
it.ucsf.edu
Published on *it.ucsf.edu* (https://it.ucsf.edu)

Home > Security Update:Significant Vulnerability SSL 3.0 Affecting All Users (Referred to as the Poodle Attack)

Security Update:Significant Vulnerability SSL 3.0 Affecting All Users (Referred to as the Poodle Attack)

Significant Vulnerability SSL 3.0 Affecting All Users (Referred to as the Poodle Attack)

Status Type

Security Update

Private

Public

Date and Time

Monday, October 20, 2014 - 16:16

Reason

Security Update

Impact

All Users

WHAT HAPPENED?

The United States Computer Emergency Readiness Team (US-CERT) reported a design flaw in encryption method known as Secure Socket Layer (SSL) 3.0. The vulnerability could allow an attacker to decrypt and extract information from inside an encrypted transaction. This is attack is known as the Poodle Attack.

While SSL 3.0 is an old encryption model and has been replaced with a more secure encryption method, most major browsers (e.g. Google Chrome, Internet Explorer) remain backwards compatible with SSL 3.0 to interoperate with legacy systems in the interest of a smooth user experience. The POODLE attack leverages the fact that when a secure connection attempt fails, servers will fall back to older protocols such as SSL 3.0.

Advanced Users: For a complete description of the vulnerabilities, affected software and updates refer to US-CERT?s Alert (TA14-290A) - SSL 3.0 Protocol Vulnerability and POODLE Attack at https://www.us-cert.gov/ncas/alerts/TA14-290A [1]

.

AFFECTED SYSTEMS:

- Any system or application that supports SSL 3.0 with CBC mode ciphers
- Most major browsers (e.g. Internet Explorer, Firefox, Chrome)

1. To check if your browser is vulnerable, run a test at poodletest.com
2. To check if a website is vulnerable, run a test at https://sslanalyzer.comodoca.com/ [2]

WHAT'S THE PROBLEM?

There's a fair chance that the POODLE flaw impacts you. Odds are good that your browser doesn?t rely on SSLv3 by default, but because of the ability to fall back to the legacy protocol when necessary, a site or server that is only configured to connect using SSLv3 will force most browsers to cater to that request.

HOW DO I PROTECT MY COMPUTER?

There is currently no fix for the vulnerability SSL 3.0 itself, as the issue is fundamental to the protocol; however, disabling SSL 3.0 support in system/application configurations is the most viable solution currently available.

- Most major browser vendors are working on disabling SSL 3.0 but it may take time for them to distribute the ?fix.?

1. If you are supported by ITFS or have different IT support, no action on your part is required.
2. If you do not have IT support or they do not support your computer, refer to your software vendor for updates or the Vulnerability Summary for CVE-2014-3566 - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566 [3].

RELATED LINKS

- Vulnerability Summary for CVE-2014-3566 - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566 [3]
- IT Security - http://it.ucsf.edu/security [4]

GET IT HELP. Contact the Service Desk online, or phone 415.514.4100

Site Login Site Index

Suggest an IT Improvement | © UC Regents

*/ //-->

referred-poodle-attack

Links
[1] https://www.us-cert.gov/ncas/alerts/TA14-290A
[2] https://sslanalyzer.comodoca.com/
[3] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
[4] http://it.ucsf.edu/security