Vulnerability in SSL 3.0 Could Allow Information Disclosure

Date: February 18, 2015
Version: 1.0
References: CVE-2014-3566

Executive Summary

A reported potential vulnerability known as SSLv3 POODLE is based on encryption technology from 1996 that is still present in current Internet browsers.

All versions of Belden's Hirschmann, Garrettcom and Tofino Security products that use web browsers for configuration use much newer versions of encryption. However, incorrect browser configuration, the use of a very old browser, or very sophisticated malware that fools the browser to incorrectly drop away from higher levels of encryption to SSL 3.0 could create an environment for this potential vulnerability to be used successfully. The user may avoid this issue by changing a setting in their internet browser.

Details

The SSL 3.0 protocol is used by Internet browsers themselves and products that are configured or monitored via browsers. Newer versions of encryption are widely used today and are known as TLS 1.0, 1.1, 1.2, etc. The SSL 3.0 protocol is still present in most Internet browsers to provide backward compatibility and is enabled by default. Furthermore, software usually utilizes the newest version of encryption possible, but still negotiates the use of earlier versions of encryption, including SSL 3.0. This is done to ensure a basic level of encryption if the newer versions are not present or enabled. SSLv3 POODLE was discovered by Google researchers in a lab environment. There are no known reported cases of SSLv3 POODLE used in industry to-date.

Impact

Successful exploitation of the vulnerability may cause a subset of the encrypted communication to be decrypted by the attacker.

Affected Products

Brand	Product Line / Platform	Product
Garrettcom	Magnum	6K, 10K, 10X, 10RX, 12K, DX
Hirschmann	Classic	RS, RSR, MACH100, MACH1000, MACH4000, MS, OCTOPUS (with software L2P and higher)
	HiOS	RSP, RSPE, RSPS, RSPL, MSP, EES, EESX
	HiSecOS	EAGLE
	Classic Firewall	EAGLE One, EAGLE mGuard
	HiLCOS	All
	Lite Managed	GECKO
	Network Management	Industrial HiVision

Suggested Actions

To prevent this potential vulnerability from being exploited, Belden recommends that users explicitly disable SSL 3.0 in the Internet browsers they use to configure Belden products. These settings are typically found in the Options or Preferences area of browsers under Advanced Settings or Security Settings. Once disabled, users should ensure that newer versions of encryption such as TLS are enabled to allow Belden products to use the newest and best encryption available. These are also enabled by default. If you have very old non-Belden applications running on your computers that may have used SSL 3.0, you can also enable earlier versions of SSL to allow those programs to continue to work. Only SSL 3.0 is affected by SSLv3 POODLE.

For Help or Feedback

To view all Belden Security Advisories and Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.eu.com and https://garrettcom-support.belden.eu.com.

Related Links

- [1] This POODLE Bites: Exploiting The SSL 3.0 Fallback

Disclaimer

THE SECURITY ADVISORY, AND INFORMATION CONTAINED HEREIN, ARE PROVIDED ON AN "AS IS" BASIS AND DO NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE ADVISORY, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE ADVISORY, IS AT YOUR OWN RISK. INFORMATION IN THIS ADVISORY AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE ADVISORIES AT ANY TIME.

Revisions

V1.0 (February 18, 2015): Advisory published.