



WatchGuard XTM Immune from Latest SSL Vulnerability

US Government identifies SSL VPN vulnerability that affects Cisco, Juniper and SonicWall

8 December 2009: WatchGuard® Technologies has confirmed that the SSL VPN technology used in its multifunction XTM (eXensible Threat Management) firewall appliances are immune from the recently discovered SSL VPN vulnerability that affects Cisco, Juniper and SonicWall.

The vulnerability, which is in essence a session hijack type of attack, is documented by the US-CERT (United States Computer Emergency Readiness Team) at <http://www.kb.cert.org/vuls/id/261869>. By convincing a user to view a specially crafted web page, a remote attacker may be able to obtain VPN session tokens and read or modify content (including cookies, script, or HTML content) from any site accessed through the clientless SSL VPN. Noted by US-CERT is the fact that this vulnerability can be used “to bypass authentication or conduct other Web-based attacks.”

Currently, there is no known fix. This makes it a worldwide critical issue because of the fact that so many remote and mobile workers use VPN connections to access internal servers for mail, file-share drives, collaboration tools and other critical applications and files.

However, all WatchGuard multifunction XTM appliances provide highly secure SSL VPN functionality and are not affected by this particular SSL problem as described by US-CERT. “As mobile workers rely on SSL VPN technology to securely connect to their remote offices or corporate networks, they need reliable connectivity solutions that are free from hackers,” said Eric Aarrestad, VP of Marketing at WatchGuard Technologies. “Unlike customers who rely on networking vendors to provide network security, WatchGuard customers can rest assured knowing that their remote and mobile employees can safely and securely connect to mission critical networks, applications and data without exposing their business to undue risks.”

The vulnerability highlighted by the US-CERT applies to SSL products that use the SSL URL rewriting technique – sometimes called URL Mangling – as a means of accessing web-based trusted resources directly from a browser. However, WatchGuard XTM appliances with SSL VPNs use an ‘access client’, which is essentially a piece of software running on an end-user’s

system that build tunnels very much the same way any IPSec VPN products do. This mechanism is not subject to this vulnerability.

More information about WatchGuard multifunction firewalls with SSL VPN capabilities is available at www.WatchGuard.com.

About WatchGuard Technologies, Inc.

Since 1996, WatchGuard® Technologies, Inc. has been the advanced technology leader of business security solutions, providing mission-critical protection to hundreds of thousands of businesses worldwide. The WatchGuard family of wired and wireless unified threat management appliances, messaging, content security and SSL VPN remote access solutions provide extensible network, application and data protection, as well as unparalleled network visibility, management and control. Marking its recent entry into the messaging and content security markets, the new WatchGuard XCS (eXtensible Content Security) platform combines innovative cloud-based security, data loss prevention and advanced messaging security technologies in a single, easy to use appliance.

WatchGuard products are backed by WatchGuard LiveSecurity® Service, an innovative support, maintenance, and education program. WatchGuard is headquartered in Seattle and has offices serving North America, Europe, Asia Pacific, and Latin America. To learn more, visit <http://www.watchguard.com/>.

###

WatchGuard is a registered trademark of WatchGuard Technologies, Inc. All other marks are property of their respective owners.

Contacts:

Natasja de Groot, WatchGuard Technologies Inc
+ 31- 70 711 2085, natasja.degroot@watchguard.com

Allie Andrews
+ 44 (0)1442 245030, allie@prpr.co.uk