Trend Micro Raises Awareness about Microsoft Windows SChannel Vulnerability

Versions dating back to Windows '95 susceptible

With the revelation of another major flaw affecting SSL/TLS, this time in Microsoft Windows Secure Channel (SChannel),Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in security software and solutions, is recommending Windows users immediately patch their systems to avoid being compromised. Windows SChannel is Microsoft's delivery platform to securely transfer data, and this potentially wormable vulnerability presents another threat to ecommerce and other critical web-based apps.

The bug, addressed in Microsoft Security Bulletin MS14-066, received a score of 10 out of 10 by the Common Vulnerability Scoring System (CVSS). Microsoft released a patch on Tuesday. Based on this classification and the propensity for attacks following potential exploit announcements, Trend Micro recommends considering using a vulnerability shielding product to provide protections while testing and deploying security updates. Trend Micro's Deep Security™ solution provides protection to combat this vulnerability.

"Similar to the well-documented Heartbleed exploit, this is yet another example of a latent vulnerability that could have far-reaching effects," said JD Sherry, vice president, technology and solutions, Trend Micro. "When news like this breaks, cyber criminals go into hyperdrive developing attacks to take advantage of the flaw. As such, it's important to quickly respond to avoid system disruption and compromise. We are urging our customers to make addressing this bug a top priority and we have provided resources accordingly to complement the latest Microsoft patches."

Trend Micro experts recommend the following action:

- Install Microsoft patches immediately
- Use a vulnerability shielding product like Deep Security to protect against attacks while testing and deploying the security update.

Trend Micro Deep Security, Deep Discovery, and Vulnerability Protection (part of Trend Micro's Smart Protection Suites) are equipped to protect enterprises against these types of attacks. Deep Security with rule DSRU14-035, Deep Discovery with rules NCIP 1.12207.00 and NCCP 1.12179.00, and Vulnerability Protection with Deep Packet Inspection (DPI) rule 1006327 covers the CVE-2014-6321 vulnerability.

A blog post is also available for additional information to help enterprises understand the ramifications of this vulnerability and how they can address this.

About Trend Micro

Trend Micro Incorporated a global leader in security software, rated number one in server security (IDC, 2013), strives to make the world safe for exchanging digital information. Built on 26 years of experience, our solutions for consumers, businesses and governments provide layered data security to protect information on mobile devices, endpoints, gateways, servers and the cloud. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™ infrastructure, and are supported by more than 1,200 threat experts around the globe. For more information, visit TrendMicro.com.
