Trend Micro Launches Free Protection for Shellshock a.k.a. Bash Bug

Preventative measures made available to all to prevent widespread outbreak

As the Shellshock a.k.a. Bash Bug continues to raise concern,Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in security software and solutions, today is taking proactive steps to mitigate adverse effects with the release of license-free tools to scan and protect servers, as well as web users, across Mac OSX and Linux platforms. The vulnerability has potential to adversely impact a half billion web servers and other Internet-connected devices including mobile phones, routers and medical devices.

"Since this situation has potential to escalate quickly, we are taking immediate preventative steps to help keep the public safe from this unprecedented vulnerability," said Eva Chen, CEO, Trend Micro. "We believe the most responsible course of action is for technology users to remain calm and apply the resources made available from Trend Micro, and others, to create a strong defensive front. By making our tools accessible free of charge to our customers, and beyond, we are trying to address this 'outbreak' to stop a possible epidemic before it can start."

Broadly publicized this week, Shellshock a.k.a. Bash Bug, is a vulnerability that can exploit command access to Linux-based systems and adversely impact a majority of the web servers around the world, as well as Internet-connected devices on the Mac OSX platform. One of the free tools featured, the on-demand BashLite Malware Scanner, will determine if the BashLite malware is resident on Linux systems.

"Shellshock could be notably more widespread than the infamous Heartbleed from earlier this year," said Raimund Genes, CTO, Trend Micro. "Heartbleed was very different in nature and behavior. With Shellshock the threats are much more severe."

Trend Micro's holistic strategy is to contain the vulnerability and build up defenses. This includes the distribution of tools to help IT administrators scan and protect servers, including web security and anti-malware tools to help protect their end-users.

To protect enterprise servers and users:

- Deep Security as a Service: This will quickly help to virtually patch vulnerable servers with updated automated protection for Shellshock.
- Deep Security for Web Apps: Used to assess web applications and detect if a server is running a web application that is susceptible to the Shellshock vulnerability.
- Deep Discovery network monitoring: Detects an attack exploiting the Shellshock vulnerability on a network and alerts IT administrators to a potential system intrusion in real time.
- Interscan Web Security: This notifies end-users of those sites that Trend Micro has identified as being affected by the Bash vulnerability.

For consumers:

- Trend Micro Free Tool for PCs, Macs and Android devices: these free tools notify the end-user of a website Trend Micro has identified as being affected by the Bash vulnerability.

The tools can be accessed here: http://www.trendmicro.com/us/security/shellshock-bash-bug-exploit/index.html.

For those unable to implement the Trend Micro wall of protection against the Shellshock threat, Trend Micro's threat defense experts recommend the following steps to help businesses and end-users mitigate the vulnerability:

- End-users should watch for patches for Mac OSX phones and implement them immediately.
- Linux system operators should consider virtually patching until a patch is available from their vendor.
- Linux/Apache webserver operators using BASH scripts should consider retooling those scripts to use something other than BASH until a patch is available.
- Hosted service customers should contact their service provider to determine if they are vulnerable and find out their remediation plans if they are exposed.

Trend Micro researchers are currently monitoring this vulnerability in the wild to anticipate additional escalations. The company's experts have also released a detailed blog post explaining the vulnerability with additional recommendations to stay protected.

Trend Micro has also created a visual FAQ-type Infographic detailing what the vulnerability is and how it works. Click here to view: http://about-threats.trendmicro.com/us/infographics/infograph/shellshock

For more information, click here:http://blog.trendmicro.com/bash-shellshock-vulnerability/.

To learn more about the free protection options offered by Trend Micro for the Shellshock vulnerability, please click

To learn more about the free protection options offered by Trend Micro for the Shellshock vulnerability, please click here:http://www.trendmicro.com/us/security/shellshock-bash-bug-exploit/index.html

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.
