February 20, 2013

Fortinet(R)'s FortiGuard(TM) Labs Discovers Critical Vulnerabilities in Adobe Shockwave Player

Affected Software Could Allow an Attacker, Who Successfully Exploits These Vulnerabilities, to Run Malicious Code on the Affected System

SUNNYVALE, CA -- (Marketwire) -- 02/20/13 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today announced the company's FortiGuard Labs has identified critical zero day vulnerabilities in Adobe Shockwave Player. Fortinet's FortiGuard Labs consist of over 175 researchers and analysts world-wide, working to discover, monitor and help protect against breaking threats. Since 2008, FortiGuard Labs has reported more than 150 zero day vulnerabilities, 124 of which have been fixed by the appropriate vendors. For a list of outstanding vulnerabilities FortiGuard has discovered that are in zero day state, please visit: http://www.fortiguard.com/advisory/UpcomingAdvisories.html.

The vulnerabilities discovered in the Adobe Shockwave Player/AIR (CVE-2013-0635 and CVE-2013-0636) could allow an attacker, who successfully exploits these vulnerabilities, to run malicious code on the affected system. They were reported in November 2012. Adobe recommends users of Adobe Shockwave Player 11.6.8.638 and earlier versions update to the newest version 12.0.0.112, available here: http://get.adobe.com/shockwave/

A zero day vulnerability is a previously unknown threat that does not yet have a patch/update available from the vendor to close the security hole, thus leaving it open to attack. Once a zero day vulnerability has been identified, it is analyzed by FortiGuard Labs and verified internally before vendors are notified. Once verified, FortiGuard Labs will develop an advanced zero day IPS signature(s) that will be deployed to customers before a vendor patch is available, which helps protect against the open security hole(s). These signatures are unique to Fortinet and play an important role in the fight against advanced persistent threats (APTs).

In addition to analyzing the threat landscape, FortiGuard Labs researchers write and present papers at global security conferences, including EICAR, Blackhat, Virus Bulletin, Insomni'Hack and Hashdays. Published papers and presentations from these shows can be downloaded from here: http://www.fortiguard.com/resources/ResearchPapers.html

Responsible Disclosure
FortiGuard Labs' responsible disclosure dictates a discovered vulnerability be patched before being disclosed to the public. Even without a working exploit or patch, a signature for the vulnerability can be generated to prevent intrusions. Once a signature is created, it is put through FortiGuard Labs' zero day signature process and assigned a generic name. The goal is to provide protection while disclosing as few details as possible. From there, FortiGuard works together with vendors to create a patch for the vulnerability. After a patch is released, FortiGuard continues to work with the vendor to analyze the source of the vulnerability and to help prevent similar zero days from being exploited in the future.

Beyond Signatures
As malware numbers have increased exponentially in recent years, network security vendors have had to find alternate methods for malware detection and mitigation. Fortinet, for example, has incorporated several new protective features and functionalities into its new operating system, FortiOS 5. FortiOS 5 includes more than 150 new security features that are designed to help protect against today's Advanced Persistent Threats (APTs) and targeted attacks. These enhancements include four key elements, which give large enterprise organizations and managed security service providers the ability to easily deploy maximum protection:

- Advanced Malware Detection: The advanced malware engine helps reduce the size and increase the performance of the malware signature database. An inline sandbox applies behavior models against a sample file to determine if it is a threat. Cloud-based inspection can then provide a more detailed analysis of suspicious files.
- Exploit Discovery and Protection: FortiOS 5 can scan and identify vulnerabilities via a network or agent scan. The intrusion protection system function can then be deployed to help protect vulnerable assets until the normal patching cycle remediates the vulnerability.
- Cloud-Based Reputation Systems: A new advanced anti-malware detection system adds an on-device, behavior-based heuristic engine and cloud-based AV services that includes an operating system sandbox and botnet IP reputation database.
- Multi-Vector Policy Engine: Although traditional policy can be applied based on source (IP address), FortiOS 5 also has the ability to apply policy based on the user and device identity. This is an important attribute for distributed, virtual and cloud networks.

Meet the FortiGuard Labs Researchers at RSA
Fortinet will be participating at the upcoming RSA security conference, which is taking place February 25 - March 1 at San Francisco's Moscone Center. Stop by booth #2025, meet the members of the FortiGuard research team, see a demonstration of the lab's latest threat intelligence services and receive a free USB wristband.

About FortiGuard Labs
FortiGuard Labs has identified the most recent threats based on data collected from FortiGate® network security appliances and intelligence systems in production worldwide. Customers who use Fortinet's FortiGuard Services should be protected against the vulnerabilities outlined in this report as long as the appropriate configuration parameters are in place.

FortiGuard Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam capabilities. These services help protect against threats on both application and network layers. FortiGuard Services are updated by FortiGuard Labs, which enables Fortinet to deliver a combination of multi-layered security intelligence and zero day protection from new and emerging threats. For customers with a subscription to FortiGuard, these updates are delivered to all FortiGate, FortiMail™ and FortiClient ™ products.

Ongoing research can be found in the FortiGuard Center or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the FortiGuard Blog.

Follow Fortinet Online: Twitter at: www.twitter.com/fortinet; Facebook at: www.facebook.com/fortinet; YouTube at: http://www.youtube.com/user/SecureNetworks.

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2012 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

FTNT-O

Rick Popko

Fortinet

408-486-7853

rpopko@fortinet.com

Source: Fortinet