Super Tuesday: A Patch Tuesday We Won’t Forget

5,026
people reacted

0

3 min. read

SHARE

By Ryan Olson

October 15, 2014 at 9:45 AM
Category: Threat Prevention, Unit 42
Tags: BlackEnergy, iSight, microsoft, Microsoft Security Bulletin, Patch Tuesday, Sandworm, vulnerability

Sometimes “Patch Tuesday” comes and goes with little excitement or fanfare; yesterday was not one of those days. In just one day, Oracle released patches for 154 new vulnerabilities, Adobe issued updates for Flash and ColdFusion, and Microsoft released 24 patches of their own. On top of the sheer volume of patches, we learned that three of the Microsoft vulnerabilities were being exploited in targeted attack campaigns.

Sandworm

The first to drop was the Sandworm Campaign, a report from iSight partners, which described attacks on European and American targets in the month of August using new versions of the BlackEnergy bot, but the group behind the attacks has been operating since at least 2009. The biggest news here was the group’s exploitation of a “new” vulnerability in Windows, CVE-2014-4114. I’m putting “new” in quotes because the vulnerability was discussed at last-month’s Virus Bulletin conference by two researchers from ESET, but without a codename like “Sandworm” it did not garner very much attention. CVE-2014-4114 exists because the Windows OLE system allows Office documents to download and execute files from remote resources (by design). Typically the execution would only happen after the user accepts a prompt indicating they want to allow the action, but when the file is a PowerPoint Show file (.pps or .ppsx) the execution occurs without any user interaction. Patches for this vulnerability are available in MS14-060.

The result of the infection is installation of the BlackEnergy malware, which has been around since 2007 but has undergone some significant development, and was also detailed by the ESET researchers at VB last month. BlackEnergy’s command and control happens over HTTP, but many of the samples related to the Sandworm campaign actually use encrypted HTTPS connections. This is yet another example of how malware uses encrypted channels to evade IPS systems and shines a spotlight on a good reason to consider enabling SSL decryption from unknown websites.

The iSight report included 10 IP addresses that have hosted Sandworm command and control servers. We dug into our WildFire system and found 24 executables from the last seven months that had contacted these servers. All of these appear to be variants of the BlackEnergy bot that connect directly to one of the 10 IP addresses, rather than resolving domain names to locate their server’s IP.

In addition to CVE-2014-4114, iSight reported four additional vulnerabilities, which the Sandworm attackers have exploited in the past. Palo Alto Networks provides the following detection signatures for these vulnerabilities and for the BlackEnergy malware.

Signature	Description	Vulnerability
36809	Windows OLE Remote Code Execution Vulnerability	CVE-2014-4114
33566	Microsoft Office RTF Parsing Stack Buffer Overflow Vulnerability	CVE-2010-3333
36193	Microsoft Windows MSCOMCTL OCX RCE Stack Buffer Overflow Vulnerability	CVE-2012-0158
36192	Microsoft Windows MSCOMCTL OCX RCE Stack Buffer Overflow Vulnerability	CVE-2012-0158
36160	Microsoft Windows MSCOMCTL OCX RCE Stack Buffer Overflow Vulnerability	CVE-2012-0158
35835	Microsoft Windows MSCOMCTL OCX RCE Stack Buffer Overflow Vulnerability	CVE-2012-0158
35506	Microsoft Windows MSCOMCTL OCX RCE Stack Buffer Overflow Vulnerability	CVE-2012-0158
35069	Microsoft Windows MSCOMCTL OCX RCE Stack Buffer Overflow Vulnerability	CVE-2012-0158
34896	Microsoft Windows MSCOMCTL OCX RCE Stack Buffer Overflow Vulnerability	CVE-2012-0158
34766	Microsoft Windows MSCOMCTL OCX RCE Stack Buffer Overflow Vulnerability	CVE-2012-0158
34753	Microsoft Windows MSCOMCTL OCX RCE Stack Buffer Overflow Vulnerability	CVE-2012-0158
36208	Microsoft Word TIFF Image Integer Overflow Vulnerability	CVE-2013-3906
36207	Microsoft Word TIFF Image Integer Overflow Vulnerability	CVE-2013-3906
36415	Microsoft Word RTF File Potential Malformed Field	CVE-2014-1761
36414	Microsoft Word RTF File Remote Code Execution Vulnerability	CVE-2014-1761
36403	Microsoft Word RTF File Remote Code Execution Vulnerability	CVE-2014-1761
13048	BlackEnergy.Gen Command and Control Traffic	N/A
12653	Bot: BlackEnergy Command and Control	N/A
13747	Bot: Win32.BlackEnergy.Botnet	N/A

CVE-2014-4113 and CVE-2014-4148

While Sandworm received the most industry attention on Tuesday, two more vulnerabilities were disclosed with less detail. CVE-2014-4113 is a privilege escalation vulnerability, reported by both FireEye and Crowdstrike. In both cases attackers have build the exploit into a Windows tool that allows them to execute other processes with System level access. Crowdstrike has attributed this tool to a Chinese cyber espionage group they have named Hurricane Panda.

Last but not least is CVE-2014-4148, which is likely the most dangerous of the bunch, and was reported by FireEye after they noticed it used in a targeted attack using a Microsoft Office file against an “international organization.” This vulnerability exists in the True Type Font (TTF) subsystem located in the win32k.sys kernel-mode driver. Exploitation of this vulnerability gives the attacker kernel-mode access, which then allows attackers to bypass restrictions placed on non-administrative users in most environments. Yesterday we released the following signature to detect this vulnerability.

Signature	Description	Vulnerability
36787	Microsoft Windows Kernel Mode Driver TrueType Font Parsing Remote Code Execution Vulnerability	CVE-2014-4148

Patches are available for both of these vulnerabilities in MS14-058 and we recommend everyone apply the patch to protect their systems. Thanks to Xin Ouyang and the entire Palo Alto Networks IPS team for making sure our customers are protected on this “Super” Patch Tuesday.