kindred

Security Newsletter

2 April 2018

Subscribe to this newsletter

Drupalgeddon2: New drupal critical security flaw, patch now!

The Drupal CMS team has fixed a highly critical security flaw that allows hackers to take over a site just by accessing an URL. Drupal site owners should immediately —and we mean right now— update their sites to Drupal 7.58 or Drupal 8.5.1, depending on the version they're running.

The Drupal team pre-announced today's patches last week when it said "exploits might be developed within hours or days" after today's disclosure. The bug —tracked under the CVE-2018-7600 identifier— allows an attacker to run any code he desires against the CMS' core component, effectively taking over the site.

The attacker doesn't need to be registered or authenticated on the targeted site, and all the attacker must do is to access an URL. The Drupal community has already nicknamed this bug as Drupalgeddon2 after the Drupalgeddon security bug (CVE-2014-3704, SQL injection, severity 25/25) disclosed in 2014 that led to numerous Drupal sites getting hacked for years afterward.

Besides fixes for Drupal's two main branches —7.x and 8.x— the Drupal team announced patches for the ancient 6.x branch that was discontinued in February 2016. Web firewall products are expected to receive updates in the following days to handle exploitation attempts. According to BuiltWith.com, Drupal currently powers over one million sites and has a 9% market share among the top 10K most popular sites.

Read More

SA-CORE-2018-002

Cisco critical flaw: At least 8.5 million switches open to attack, so patch now

Cisco has released patches for 34 vulnerabilities mostly affecting its IOS and IOS XE networking software, including three critical remote code execution security bugs. Perhaps the most serious issue Cisco has released a patch for is critical bug CVE-2018-0171 affecting Smart Install, a Cisco client for quickly deploying new switches for Cisco IOS Software and Cisco IOS XE Software.

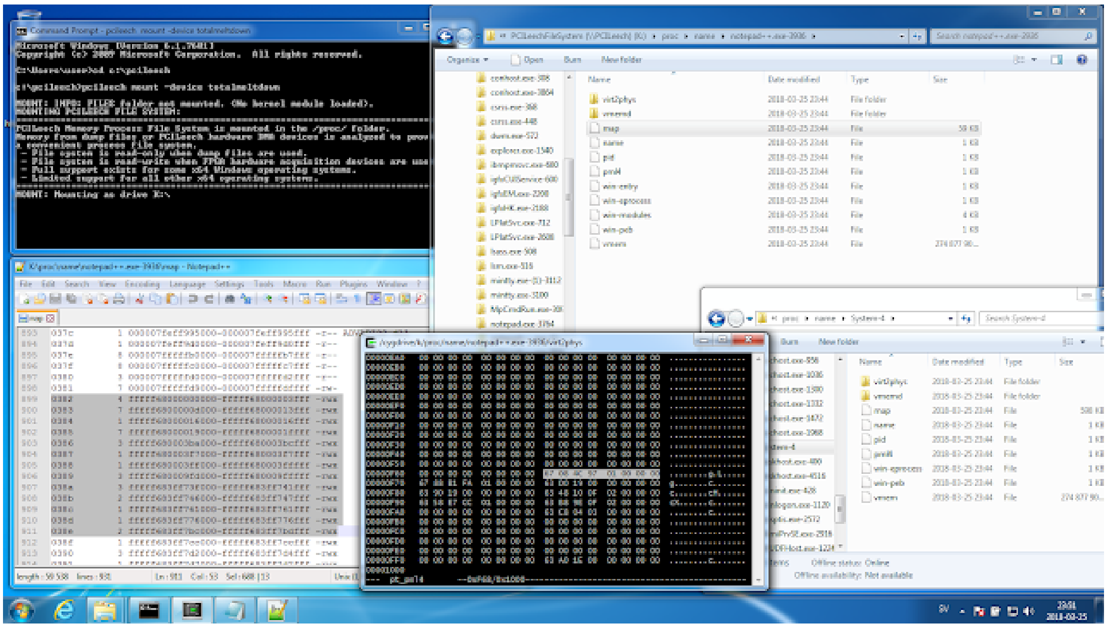
A remote unauthenticated attacker can exploit a flaw in the client to reload an affected device and cause a denial of service or execute arbitrary code. Embedi, the security firm that found the flaw, initially believed it could only be exploited within an enterprise's network. However, it found millions of affected devices exposed on the internet.

Smart Install is supported by a broad range of Cisco routers and switches. The high number of devices with an open port is probably because the Smart Install client's port TCP 4786 is open by default. This situation is overlooked by network admins, Embedi said. The company has also published proof-of-concept exploit code, so it probably will be urgent for admins to patch.

Read More

CVE-2018-0171

Windows 7 Meltdown patch opens worse vulnerability: Install March updates now



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\user>cd c:\pcileech

c:\pcileech>pcileech mount -device totalmeltdown

MOUNT: INFO: FILES folder not mounted. (No kernel module loaded).
MOUNTING PCILEECH FILE SYSTEM:
===============================================================================
PCILeech Memory Process File System is mounted in the /proc/ folder.
Memory from dump files or PCILeech hardware DMA devices is analyzed to prov
a convenient process file system.
 - File system is read-only when dump files are used.
 - File system is read-write when FPGA hardware acquisition devices are use
 - Full support exists for some x64 Windows operating systems.
 - Limited support for all other x64 operating systems.
===============================================================================
MOUNT: Mounting as drive K:\
```

K:\proc\name\notepad++.exe-3936\map - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
PCILeechFileSystem (\\PCILeech) (K:) ▸ proc ▸ name ▸ notepad++.exe-3936 ▸
Search notepad++.exe-3936
Organize ▾ Open Burn New folder

Name	Date modified	Type	Size
virt2phys	2018-03-25 23:44	File folder	
vmemd	2018-03-25 23:44	File folder	
map	2018-03-25 23:44	File	58 KB
name	2018-03-25 23:44	File	1 KB
pid	2018-03-25 23:44	File	1 KB
pml4	2018-03-25 23:44	File	1 KB
win-entry	2018-03-25 23:44	File	1 KB
win-eprocess	2018-03-25 23:44	File	1 KB
win-modules	2018-03-25 23:44	File	4 KB
win-peb	2018-03-25 23:44	File	1 KB
vmem	2018-03-25 23:44	File	274 877 90...

Microsoft's early patches for Intel's Meltdown CPU vulnerability created an even bigger problem in Windows 7 that allowed any unprivileged application to read kernel memory.

Microsoft's January and February patches stopped the Meltdown bug that exposed passwords in protected memory, but security researcher Ulf Frisk has discovered that the patches introduced a far worse kernel bug, which allows any process to read and write anywhere in kernel memory.

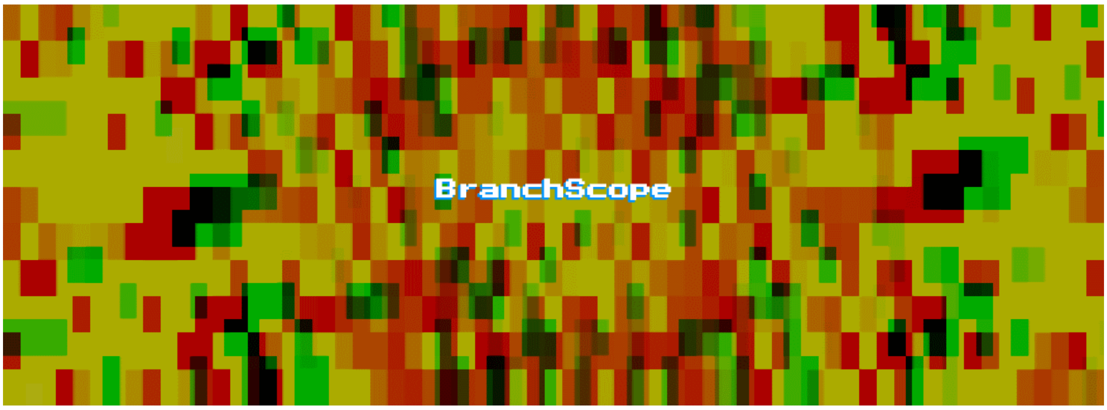
Frisk says the bug would be "trivially easy" to use to access all physical memory on. This issue affected only 64-bit versions of Windows 7 and Windows Server 2008 R2. We say affected because Microsoft patched the bug by flipping the PML4 permission bit back to its original value in this month's Patch Tuesday. Windows 7 and Server 2008 R2 users should make sure they installed both the January 2018 and March 2018 Patch Tuesday releases. Windows 10 or 8.1 systems were never affected or put at risk. Physical access is required to exploit the bug

Read More

Even More

Original statement from PCILeech creator

Academics Discover New CPU Side-Channel Attack Named BranchScope



A team of academics from four US universities have discovered a new side-channel attack that takes advantage of the speculative execution feature in modern processors to recover data from users' CPUs. Researchers named this new technique BranchScope because it attacks the "branch prediction" operation —which is the same part of a CPU speculative execution process that the Spectre variant 2 (CVE-2017-5715) vulnerability also targets.

Spectre 2 has provoked both operating system and hardware changes, with more hardware fixes planned. The researchers suggest that a similar combination of solutions would be needed for BranchScope; some software can be modified to eliminate branches, and hardware could be altered to partition the speculative execution data structures on the processor so that one process could not attack another.

Besides Meltdown, Spectre, and now BranchScope, other side-channel attacks recently discovered include SgxSpectre, MeltdownPrime and SpectrePrime. It's likely to be years before researchers have determined all the various ways in which the speculative execution hardware can be used to leak information this way, and it will be longer still before robust, universal defenses are available to stop the attacks.

Read More

More branch prediction processor attacks are discovered

The CLOUD Act — A needed fix for U.S. and foreign law enforcement or threat to civil liberties?

The United States Congress passed late last night a $1.3 trillion budget spending bill that also contained a piece of legislation that allows internal and foreign law enforcement access to user data stored online without a search warrant or probable cause. The legislation is the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), a bill proposed in mid-February.

The CLOUD Act would amend the SCA to require service providers to “preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.” The CLOUD Act would also give “qualifying” foreign governments access to records stored in the U.S. that pertain to foreign citizens, including foreign citizens here in the U.S.

it is not clear whether the bill, in its current form, would meet legal requirements under the EU’s impending General Data Protection Regulation Act. Article 48 of the GDPR addresses foreign (including U.S.) investigations and prohibits the transfer or disclosure of personal data unless pursuant to an MLAT or other international agreement. One possible resolution would be for the U.S. to enter into an agreement with the EU or for the EU to agree that the U.S. investigations and subsequent transfers or disclosures in compliance with the CLOUD Act procedures do not conflict with Article 48.

Read More

Even More

Cutting room floor

- Omitting the “o” in .com Could Be Costly
- Unmasking Monero: stripping the currency’s privacy protection
- 1Password nets partnership with ‘Have I Been Pwned’
- Stingray spying: 5G will protect you against surveillance attacks, say standards-setters
- IETF Approves TLS 1.3
- Introducing XSS Auditor reporting to Report URI
- Carbanak: Mastermind behind EUR 1 Billion cyber bank roberry arrested in spain

#Tech and #Tools

- QubeOS 4.0 has been released!
- New Site Resurrects CrackMe Challenges From the Old Crackmes.de
- Discovering Smart Contract Vulnerabilities with GOATCasino
- Forgot About Default Accounts? No Worries, GoScanSSH Didn’t

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us