The biggest security hole in 2018

2018 is a year of headache for global IT professionals.

2018 is a year of headache for global IT professionals.There have been many major security holes, even related to the hardware level faced by information security experts.Here are the four biggest vulnerabilities of 2018 and how you can use them to deal with them.

Specter and Meltdown - who dominate security projects throughout 2018

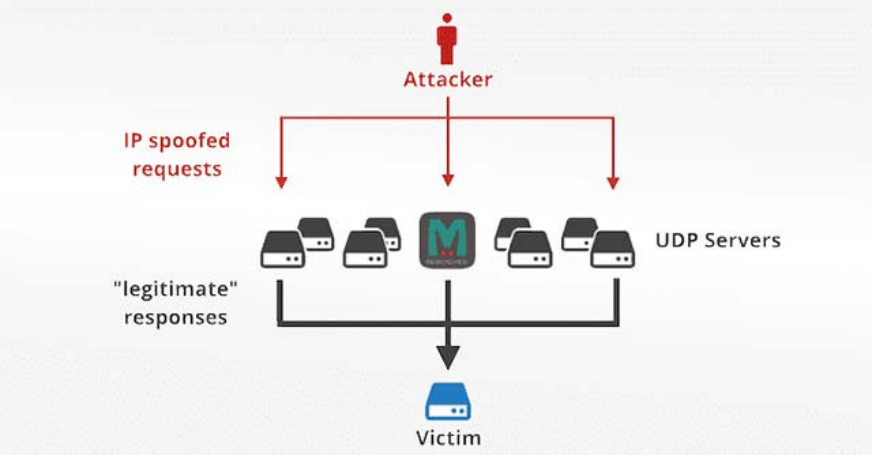
First appeared on January 4, 2018, Specter and Meltdown vulnerabilities allowed applications to read kernel memory and caused serious security problems for IT professionals during the remaining months. of year.The problem lies in the fact that the duo represents hardware-level vulnerabilities, which can be minimized, but cannot be patched via software.Although Intel processors (except for Atom chips manufactured before 2013 and Itanium series) are the most vulnerable, microcode patches are still needed for both AMD processors. OpenPOWER and other CPUs are based on Arm design.Some software remedies can also be implemented, but they often require suppliers to recompile their programs with on-the-spot protection measures.

Revealing the existence of these loopholes has caused a new interest in side-channel attacks that require a bit of deductive manipulation.Months later, the BranchScope vulnerability was also revealed.Researchers behind the findings pointed out that BranchScope provides data readability that needs to be protected by SGX safety zones, as well as defeating ASLR.

In summary, along with the original revelations, Specter-NG, Specter 1.2 and SpectreRSB, there were a total of eight variations of the Specter vulnerability discovered, besides other related vulnerabilities such as SgxPectre.

1. List of links to download BIOS updates for Meltdown and Specter

DDoS attacks break records with memcached



In 2018, hackers organized DDoS attacks using vulnerabilities in memcached, reaching 1.7Tbps.The attack is initiated by a server spoofing its own IP address (specifying the address of the attack destination as the root address), and sending a 15-byte request packet - answered by a machine memcached owners are vulnerable to feedback from 134KB to 750KB.The size difference between requests and feedback is greater than 51,200 times making this attack particularly powerful!

Proof-of-concept - a type of code that can be easily modified with attacks launched by many different researchers to deal with this situation, among them "Memcrashing.py", is credited with Match with the Shodan search engine to find vulnerable servers where an attack can be started.

Fortunately, it is possible to prevent DDoS memcached attacks, however, memcached users should also change the default settings to prevent their system from being abused.If UDP is not used in your system, you can turn this feature off with the -U 0. switch. Otherwise, limiting access to localhost with -listen conversion is 127.0.0.1.

The Drupal CMS vulnerability allows an attacker to control your site

Emergency patches for 1.1 million Drupal websites had to be released by the end of March. This vulnerability is related to conflict between how PHP handles arrays in URL parameters, and the use of hash functions. (#) of Drupal at the beginning of array keys to denote special keys often leads to additional calculations, which may allow an attacker to 'inject' the code arbitrarily.The attack nicknamed "Drupalgeddon 2: Electric Hashaloo" by Scott Arciszewski came from the initative Paragon.

In April, incidents related to this vulnerability were patched a second time, aimed at the ability to handle the URL of GET parameters to delete the # symbol, which could cause remote code execution vulnerabilities.

Although the vulnerability has been publicly warn, there are still more than 115,000 Drupal sites affected and many botnets actively take advantage of the flaw to deploy malicious encryption software.

BGP attacks block DNS servers to steal addresses

The Border Gateway Protocol (BGP), the 'tool' used to determine the most efficient path between two systems on the internet, is expected to be the target of future toxic agents by the protocol. Most design before the malicious network problems are carefully considered.There is no centralized right for BGP routes and ISP-approved routes, placing it beyond the reach of typical enterprise scale models and also out of reach. of the user.

In April, a BGP attack was conducted against Amazon Route 53 - AWS DNS service component.According to Oracle's Internet Intelligence team, the attack stems from hardware placed in a facility run by eNet (AS10297) in Columbus, Ohio, USA.Attackers redirected requests to access MyEtherWallet.com to a server in Russia, which used a phishing site to copy account information by reading existing cookies.The hackers earned 215 Ether from this attack, equivalent to about $ 160,000.

BGP has also been abused by some state organizations in some cases.In November 2018, reports indicated that some organizations in Iran had used BGP attacks to try to block the traffic of Telegram to the country.In addition, China has been accused of using BGP attacks through points present in North America, Europe and Asia.

The work of protecting BGP against these attacks is being undertaken by NIST and DHS Science and Technology Directorate, in partnership with Secure Inter-Domain Routing (SIDR), which aims to "authenticate BGP origin sources (BGP Route Origin Validation) using the Resource Public Key Infrastructure.

See more:

1. The top 3 multicloud security challenges and how to build strategies
2. How to check if the computer network is safe
3. How do I know if someone has accessed and used your computer?
4. Top 10 best free Keylogger software with Windows

You finished reading the article "**The biggest security hole in 2018**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
