IT Report

By

Ngoc Nguyen

There always are such threats and risks that affect the most robust operating systems, and Windows is not an exception to vulnerabilities that can be used (with all the bad intentions) to exploit. A few days ago has come to light the latest Windows vulnerability, which affects it and puts at risk all those PCs that have Windows (Warren, 2019). This vulnerability has its origin in the Windows Task Scheduler, specifically in the ALPC (Advanced Local Procedure Call). Other users have also investigated and confirmed that the 64-bit versions of even Windows 10 still have the bug. Microsoft recommends all its users and administrators to update their operating system as soon as possible so as not to be a victim more for these vulnerabilities. One of the Vulnerabilities found is the zero-day Exploitation of Vulnerability in which it is tracked as CVE-2018-8589; it was detected and exploited in real scenarios by multiple groups of persistent advanced threats.

The other vulnerability was related to BitLocker Security. It is present when Windows suspends BitLocker device encryption, which can allow an attacker physical access to a shutdown system and bypass security and obtain access to encrypted data (Cimpanu, 2019).

How to mitigate vulnerabilities?

Having an anti-exploit program can help protect from serious attacks. There should be an adaptive defense advanced cybersecurity solution which should include dynamic exploit detection, which serves to protect web browsers and their plug-ins, as well as other components installed on the computer.

Maximize the precautions about the files that we download from non-security sources in the network or by physical means.

There should be multi-layered protection that responds to a comprehensive security strategy, which is not based solely on a single type of software or technology.

 Vulnerabilities of Hypervisor

Recently a report of the Cloud Security Alliance has been published highlighting the main threats or security problems that can be found in the use of cloud computing. Some hypervisors on a server or a workstation are vulnerable to attacks through system firmware. Hypervisors work as the piece of software that runs directly on the hardware and controls all virtual images-everything that allows the operation of a machine and communication, among others. The detected attacks guided a successful installation of a rootkit in the system firmware (such as a BIOS), leaving hypervisor accesses vulnerable and exposing the memory content of the same (Huang & Wu, 2018).

Hypervisors employ a series of techniques to isolate the software and thus protect the secrets of each machine, including its operating systems. However, these protections are limited when the system firmware of the physical machine is infected with a rootkit. In this specific attack case, the firmware rootkit was installed by reprogramming the system firmware. This is because operating systems tend to create an "administrative guest" account, which has limited resources and can be used by the same administrator as a "back door" to access the system. These accounts are usually created with default keys that are very simple like "password," "guest," and it is usual for administrators to forget to disable it or make more complex access codes or establish some control over that account. These "back doors" are used by hackers, who will insist on their search to access a vulnerable system and achieve control of it.

This is why it will be essential to take the necessary precautions to strengthen the security of the systems of the organizations.

Solutions and vulnerabilities

The obvious solution is to increase the protection in the firmware. However, our research also showed that an attacker could take advantage of other vulnerabilities if the hypervisor allows direct access to the firmware interfaces. That is why an immediate measure will be to disable the accounts of "administrative guests" that create the operating systems by default or create a new, more robust password for this account.

To take an exhaustive control of the environment to detect activities and unauthorized changes both in the usual tasks and processes and in the data stored in the virtualized systems.

Promote very strict authentication and access controls for accessing and performing administrative operations.

Perform vulnerability analysis and configuration audits regularly.

To conclude, it is worth noting the importance that cloud computing is currently charging, so detecting and resolving these and other threats is crucial to adapt to the user's security needs, and provide the service with the necessary guarantees in this matter.

Vulnerabilities of Apache 2.X

Apache has launched a warning after discovering multiple vulnerabilities that put users at risk. They urge to update HTTP Apache servers as soon as possible. These vulnerabilities affect many versions of Apache 2.4, and users should update version 2.4.39 as soon as possible. As we always indicated, it is very important to have the systems updated and with the latest security patches to avoid suffering any type of attack (Chauhan, 2018).

Six important vulnerabilities that affect Apache HTTP servers are

In total, six vulnerabilities have been detected that affect the Apache HTTP Server. Three of them have been considered as high severity, while the rest have been classified as low.

One of the vulnerabilities has been named CVE-2019-0211. This code is executed in secondary processes or sub-processes with few privileges. In case they managed to exploit this vulnerability, it would allow an attacker to execute arbitrary code (Rudis, 2019).

Another vulnerability has been identified as CVE-2019-0217. In this case, it would allow a possible attacker who has the necessary credentials to be able to authenticate with another username. I could thus omit access control restrictions.

The third and last vulnerability that they have classified as high severity has been called CVE-2019-0215. In this case, it is an error in mod\_ssl. This time it could allow an attacker to circumvent access control restrictions. This attacker has to support Post-Handshake authentication.

It should be mentioned that these are the three vulnerabilities that have been indicated as more serious. However, as we have seen, there are three others of less importance. These vulnerabilities have been named CVE-2019-0197, CVE-2019-0196, and CVE-2019-0220.

It is important to download all kinds of files from official sources. In this way, we avoid software that could have been modified maliciously. In the official website of Apache, they show us the link to securely download the official files for the installer for the Windows operating system. Here we can also find the official document where they indicate the necessary steps. What we do next is unzipped the file in the same directory where it was previously installed. We can simply change the name to the previous directory and in this way have a backup in case of any problem, as they inform us in this web.

In short, they have detected serious vulnerabilities that affect the Apache HTTP server. Our advice is to update as soon as possible. It should be mentioned that in addition to correcting security problems, with each update, there are usually some improvements in functionality. Therefore, we always advise keeping the latest versions installed. Not only for safety but to have the latest performance improvements available.

Vulnerabilities of PHP

The two most important vulnerabilities on the Internet are as under

1. Unvalidated parameters

The most important thing at this point is to deactivate the register globals. This configuration setting is disabled by default as of PHP 4.2.0.

2. Vulnerabilities in the management of accounts and sessions

Use the built-in functions in PHP to manage sessions. However, be careful with the configuration of the server and how it stores the session information. For example, if the content of the session is stored as files in / tmp, any user who accesses the records on the server can see the content of all the sessions. Stores sessions in a database or in a part of the file system that only web administrators can access.

Software and Hardware components to protect Zeus website

WAF stands for Web Application Firewall and is a security measure that protects websites from attacks that exploit web application vulnerabilities. It is installed in front of the Web server to analyze and inspect the communication, protect the Web site from such attacks, and is used in the role to prevent unauthorized login.

Like online banking and shopping sites, it is suitable for protecting websites that have built-in applications, such as accepting user input and dynamically generating pages upon request.

According to a report, many of the compromised websites used CMS such as WordPress. The CMS security measures include the following:

1. Keep CMS up-to-date (including extensions)

2. Access restriction of management page

3. Protection of login page

4. Introduce.WAF (Protection against attacks exploiting web application vulnerabilities)

5. Antivirus measures

6. Proper configuration of SSH / FTP

To reduce the risk of web falsification caused by attacks, total security measures, including WAF, are required.

Precautionary measures when it is difficult to correct the vulnerability.

Even if you know the existence of the vulnerability, you can use the WAF if you cannot fix the web application immediately. In some cases, the in-house development system cannot be established, or the development source has left the business. Also, if a vulnerability is found in the open source software you are using, it is effective to prevent it with the WAF because you cannot directly participate in the correction.

In Web sites, there are usually multiple URLs to monitor. It is not realistic to keep monitoring many URLs 24/7 by human power. Hiring personnel for monitoring and outsourcing monitoring services can be costly. To solve this problem, many web administrators use monitoring tools to automate URL monitoring.

A tool that makes it easy to get started with URL monitoring the Zeus Book server

Applications Manager provided by Manage Engine is one of the tools that can easily start URL monitoring. You can monitor URLs and automatically obtain information such as accessibility, response time, and page size for easy visualization.

You can automatically check whether your website or web application is working properly.

You can check if there is any change in the web page, Informs administrators of connection problems, slow page loads, content errors and more, automatically calculate and create website performance reports, Monitor web pages for error messages.

**References**

Chauhan, B. (2018). 3 Most Critical Apache Vulnerabilities Found - Astra Web Security Blog. Retrieved from https://www.getastra.com/blog/911/top-3-most-critical-apache-vulnerabilities-found/

Cimpanu, C. (2019). New BitLocker attack puts laptops storing sensitive data at risk | ZDNet. Retrieved from https://www.zdnet.com/article/new-bitlocker-attack-puts-laptops-storing-sensitive-data-at-risk/

Huang, D., & Wu, H. (2018). Hypervisor-Based Virtualization - an overview | ScienceDirect Topics. Retrieved from https://www.sciencedirect.com/topics/computer-science/hypervisor-based-virtualization

Labs, M., Davis, G., Davis, G., & Sarang, R. (2015). Vulnerable From Below: Attacking Hypervisors Using Firmware And Hardware | McAfee Blogs. Retrieved from https://securingtomorrow.mcafee.com/other-blogs/executive-perspectives/vulnerable-from-below-attacking-hypervisors-using-firmware-and-hardware/

Rudis, B. (2019). Apache HTTP Server Privilege Escalation (CVE-2019-0211) Explained. Retrieved from https://blog.rapid7.com/2019/04/03/apache-http-server-privilege-escalation-cve-2019-0211-what-you-need-to-know/

The vulnerabilities of hypervisors. (2019). Retrieved from https://www.techadvisory.org/2019/04/the-vulnerabilities-of-hypervisors/

Warren, T. (2019). Microsoft warns 1 million computers are still vulnerable to major Windows security exploit. Retrieved from https://www.theverge.com/2019/5/31/18647646/microsoft-windows-1-million-machines-bluekeep-remote-desktop-security-exploit