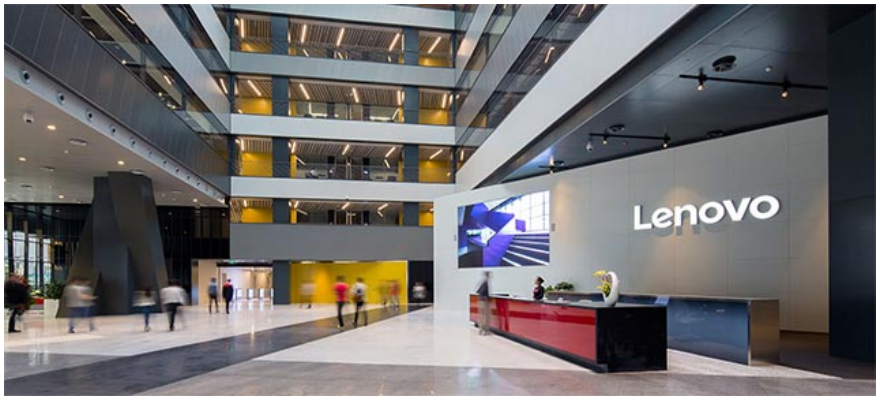
Detects many security vulnerabilities in Lenovo server infrastructure

There are a total of 9 different security holes found in Lenovo's server infrastructure.

Security researchers have recently discovered the presence of multiple vulnerabilities from simple to dangerous in Lenovo's server infrastructure. These vulnerabilities, if successfully exploited, will seriously damage the security and integrity of Lenovo's systems.

More specifically, researchers from Swascan, an Italian-based cyber security company, have discovered many vulnerabilities exist on Lenovo systems. If an attacker can exploit these vulnerabilities, it will cause many complex problems on the company's system, including arbitrary code execution behavior, and the occurrence of system problems that affect directly. Next to customers.

1. Overview of building enterprise security detection and response system



There have been 9 medium to serious vulnerabilities found in Lenovo's system

According to information posted on the Swascan personal blog, there were a total of nine different security holes found in Lenovo's server infrastructure. In particular, there are 2 cases that are classified as particularly serious, which can lead to high security risks, and 7 vulnerabilities are rated at an average level.

The researchers did not specify details of the discovered vulnerabilities. However, they shared some relatively important information regarding the nature of these vulnerabilities through CWE numbers. The recorded vulnerabilities include limited errors that operate incorrectly in the buffer memory limit, NULL Pointer Pereference, incorrect input validation, and neutralizing incorrectly used special elements in the OS command, false authentication errors . These vulnerabilities can basically allow an attacker to execute arbitrary code, read sensitive information and trigger remote system problems.

1. Botnet Echobot spreads across a wide range, specifically targeting Oracle and VMware applications

Lenovo patched the flaw

Immediately after discovering the above errors, Swascan researchers promptly informed the security - security department of Lenovo. With the help of the Italian security group, Chinese technology equipment manufacturers have successfully patched the gaps that seriously affect the availability, integrity and security of systems. .

Observers and security experts appreciate the agility and seriousness of Lenovo security team in dealing with vulnerabilities before they can leave the consequences. On the personal blog, the Swascan group made the following comments:

"Lenovo has shown seriousness and absolute focus on our findings. Along with email exchange, analysis, situation assessment and planning to fix problems almost immediately. immediately, it is not surprising that they can handle the vulnerabilities so quickly, it can be said that Lenovo owns the most serious, professional and transparent security team we have ever witnessed and collaborated with. ".

In addition, the researchers did not forget to emphasize the importance of good cooperation between the security research group and the supplier in timely handling of all security incidents.

1. Find out about Ghidra - NSA's powerful cybersecurity tool

In April, the Swascan group also pointed out the existence of various vulnerabilities in Microsoft server infrastructure that could allow arbitrary code execution when successfully exploited by exploiters. Previously, researchers also shared their findings regarding serious security vulnerabilities in Adobe IT systems and were highly appreciated.