The US shares the top 20 vulnerabilities most exploited by Chinese hackers since 2020 until now

NSA, CISA and FBI have just released a list of vulnerabilities most exploited by Chinese hackers to target government and critical infrastructure networks.

NSA, CISA and FBI have just released a list of vulnerabilities most exploited by Chinese hackers to target government and critical infrastructure networks.

Three federal agencies say that Chinese-sponsored hackers are targeting American and allied technology companies and networks to access sensitive networks and steal intellectual property.

"NSA, CISA and FBI continue to assess cyberattacks conducted by Chinese hackers as one of the largest and most dynamic threats to U.S. government and civilian networks," the security consultancy said . The general secret of the three agencies is clearly stated.

This new advisory builds on previous reports from NSA, CISA, and FBI to inform federal and state, local, tribal, and territorial (SLTT) governments; critical infrastructure, including the Defense Industrial Base Park; and private sector organizations on notable trends and long-standing tactics, techniques, and procedures (TTPs).

The consultancy also provides recommended mitigation measures for each security vulnerability most exploited by Chinese hackers as well as detection methods and vulnerable technologies for security units to detect and prevent. block future attacks.

According to the NSA, CISA and FBI, the following security holes have been exploited the most by Chinese hackers from 2020 up to now:

The firm	CVE	Vulnerability type
Apache Log4j	CVE-2021-44228	Remote Code Execution (RCE)
Pulse Connect Secure	CVE-2019-11510	Arbitrary file reading (AFR)
GitLab CE/EE	CVE-2021-22205	Remote Code Execution (RCE)
Atlassian	CVE-2022-26134	Remote Code Execution (RCE)
Microsoft Exchange	CVE-2021-26855	Remote Code Execution (RCE)
F5 Big-IP	CVE-2020-5902	Remote Code Execution (RCE)
VMware vCenter Server	CVE-2021-22005	Arbitrary file reading (AFR)
Citrix ADC	CVE-2019-19781	Path Traversal
Cisco Hyperflex	CVE-2021-1497	Command Line Execution (CLE)
Buffalo WSR	CVE-2021-20090	Relative Path Traversal
Atlassian Confluence Server and Data Center	CVE-2021-26084	Remote Code Execution (RCE)
Hikvision Webserver	CVE-2021-36260	Command Injection (CI)
Sitecore XP	CVE-2021-42237	Remote Code Execution (RCE)
F5 Big-IP	CVE-2022-1388	Remote Code Execution (RCE)
Apache	CVE-2022-24112	Spoofing bypasses authentication
ZOHO	CVE-2021-40539	Remote Code Execution (RCE)
Microsoft	CVE-2021-26857	Remote Code Execution (RCE)
Microsoft	CVE-2021-26858	Remote Code Execution (RCE)
Microsoft	CVE-2021-27065	Remote Code Execution (RCE)
Apache HTTP Server	CVE-2021-41773	Path Traversal

Mitigation measures

NSA, CISA and FBI also urge US governments and allies, critical infrastructure and private sector organizations to adopt the following mitigation measures to defend against attacks by Chinese hackers cause.

The three federal agencies advise organizations to install security patches as soon as possible, use anti-phishing multi-factor authentication (MFA) whenever possible, and replace existing infrastructure. Using software that is no longer updated for security.

They also advise everyone to move to a Zero Trust security model and enable strict logging on internet-exposed services to detect attacks as early as possible.