Analysis of CISA releases Advisory on Top CVEs Exploited Chinese State-Sponsored Groups

securityboulevard.com/2022/10/analysis-of-cisa-releases-advisory-on-top-cves-exploited-chinese-state-sponsored-groups/

by Flashpoint Team on October 7, 2022

October 7, 2022

CISA advisory

On October 6, 2022, the US Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) released a joint advisory, AA22-279A, identifying twenty of the top vulnerabilities that have been actively exploited by Chinese state-sponsored cyber actors since 2020. The actors leveraged virtual private networks (VPNs) to obfuscate the source of the exploitation activity and then conducted lateral movement within the target networks.

Over the same time period, Flashpoint analysts have observed the majority of these vulnerabilities being heavily mentioned among threat actors, especially in Russian-language hacking and exploit forums. Seventeen out of the twenty CVE IDs (listed below) have been among the monthly most mentioned vulnerabilities in Flashpoint's collections. **This indicates that while CISA has attributed attempts to exploit these CVEs to China, they are likely also being heavily targeted by threat actors of other regions**. This is because the exploits targeting these vulnerabilities are simple to use and reliable, and there are high incentives to exploitation.

Flashpoint has made the following insights into the most noteworthy targeted vulnerabilities using VulnDB database.

Log4Shell and ProxyLogon

A majority of the vulnerabilities covered by the advisory are among the major vulnerabilities disclosed during the last few years—those that have repeatedly made the news due to their widespread exploitation. These include Log4Shell (VulnDB 275958), the vulnerability in the Apache Log4j, and ProxyLogon (VulnDB 250803), which encompasses four Microsoft Exchange issues.

CVE-2021-22204 and CVE-2021-22205

Another notable set of vulnerabilities on the list is **CVE-2021-22204** and **CVE-2021-22204** (VulnDB 254347), which was disclosed on April 13, 2021, and describes an issue in ExifTool that allows for arbitrary code execution. The vulnerable code is in a library, meaning it may not be straightforward to exploit, depending on implementation. It is not common to see this type of tool or library appear on such a list—as opposed to tools such as Apache Log4j, which, while also a library, is designed to handle input from a remote source.

Flashpoint also notes some inconsistencies in the CVE identification and severity level of these vulnerabilities. The National Vulnerability Database (NVD) treats this as two issues, while Flashpoint assesses that the two CVEs are a duplicate. NVD scores CVE-2021-22204 as CVSSv3 7.8 while quoting the vendor score as 6.8. The second CVE, CVE-2021-22205, is given just the vendor's score, which is CVSSv3 10.0—causing unnecessary confusion for organizations using NVD CVSS scoring to do vulnerability triage. Flashpoint and RBS assess that CVSSv3 7.8 score is accurate, but our score makeup differs from both NVD and the vendor despite the number being equivalent.

CVE-2021-36260

Another vulnerability of interest is **CVE-2021-36260** (VulnDB 268325), a remote command execution flaw in multiple **Hikvision** products. This vulnerability has previously been seen exploited by "Moobot," but is not widely associated with advanced persistent threat (APT) activity. The vulnerable Hikvision web server resides within Hikvision's IP camera devices as well as network video recorder devices, which are designed to be network accessible and operate around the clock. The vulnerability enables remote code execution without any authentication or user interaction, greatly simplifying the exploitation process. Further, Hikvision products are ubiquitous among both home users and small businesses, providing a large number of potentially vulnerable devices over the internet. These factors make this vulnerability ideal for developing botnets.

This vulnerability is also notable because it has a complete disclosure timeline: While it took the vendor two days to respond to the direct report, it took ninety days to patch and an additional thirty-six days before a public exploit was seen. NVD scores this as CVSSv2 9.3, while Flashpoint and RBS score it as 10.0.

CVE-2022-26134

The newest vulnerability on the list is **CVE 2022-26134** (VulnDB 291802), disclosed on June 2, via active exploitation in the wild. It is a flaw in Atlassian Confluence Server related to OGNL content handling, leading to remote code execution. It is known to be included in commercial exploit frameworks and exploited in cryptojacking campaigns, and according to VulnDB it has been exploited by several threat actors, including DEV-0401 and DEV-0234, both attributed to China.

EPSS SCORES

The current Exploit Prediction Scoring System (EPSS) scores for these vulnerabilities, according to the Forum of Incident Response and Security Teams (FIRST), is as follows.

CVE ID	EPSS Score (Percentage)
CVE-2021-44228	90.48%
CVE-2019-11510	96.51%
CVE-2021-22205	69.87%
CVE-2022-26134	86.38%
CVE-2021-26855	96.21%
CVE-2020-5902	96.82%
CVE-2021-22005	92.03%
CVE-2019-19781	95.61%
CVE-2021-1497	1.06%
CVE-2021-20090	1.06%
CVE-2021-26084	96.20%
CVE-2021-36260	87.79%
CVE-2021-42237	93.64%
CVE-2022-1388	91.51%
CVE-2022-24112	69.87%
CVE-2021-40539	95.95%
CVE-2021-26857	31.09%
CVE-2021-26858	31.09%
CVE-2021-27065	61.80%
CVE-2021-41773	92.45%

Manage vulnerabilities with Flashpoint

Thousands of vulnerabilities are identified every year, and the exploitation of them has dramatically increased. Organizations have even less time than before to respond to critical issues. To better protect your network, enterprises need to proactively manage risk in a timely manner. **Sign up for a free trial** and see how quality intelligence empowers a vulnerability risk management program, allowing your security teams to prioritize and remediate what really matters.

Begin your free trial today.

The post Analysis of CISA releases Advisory on Top CVEs Exploited Chinese State-Sponsored Groups appeared first on Flashpoint.

*** This is a Security Bloggers Network syndicated blog from Threat Intelligence Blog | Flashpoint authored by Flashpoint Team. Read the original post at: https://flashpoint.io/blog/cisa-releases-advisory-on-top-cves-exploited-chinese-state-sponsored-groups/