TOKIO MARINE HCC

Prioritize What Matters

Cyber & Professional Lines Group

Surviving Highly Targeted, Internet-Facing Vulnerabilities

At **Tokio Marine HCC – Cyber & Professional Lines** Group (CPLG), we continuously perform analyses and review of ransomware claims to ensure our policyholders are aware of some of the most widely leveraged vulnerabilities exploited by ransomware groups. Our CTI (Cyber Threat-Intelligence) team tracks current attack patterns and exposures by scanning customers' external networks, observing honeypot activity and malware logs, and by monitoring sales and chatter in underground markets.

The team performs periodic, non-intrusive active scans, and provides mitigation support should an active exposure of concern be detected on the insured's network.

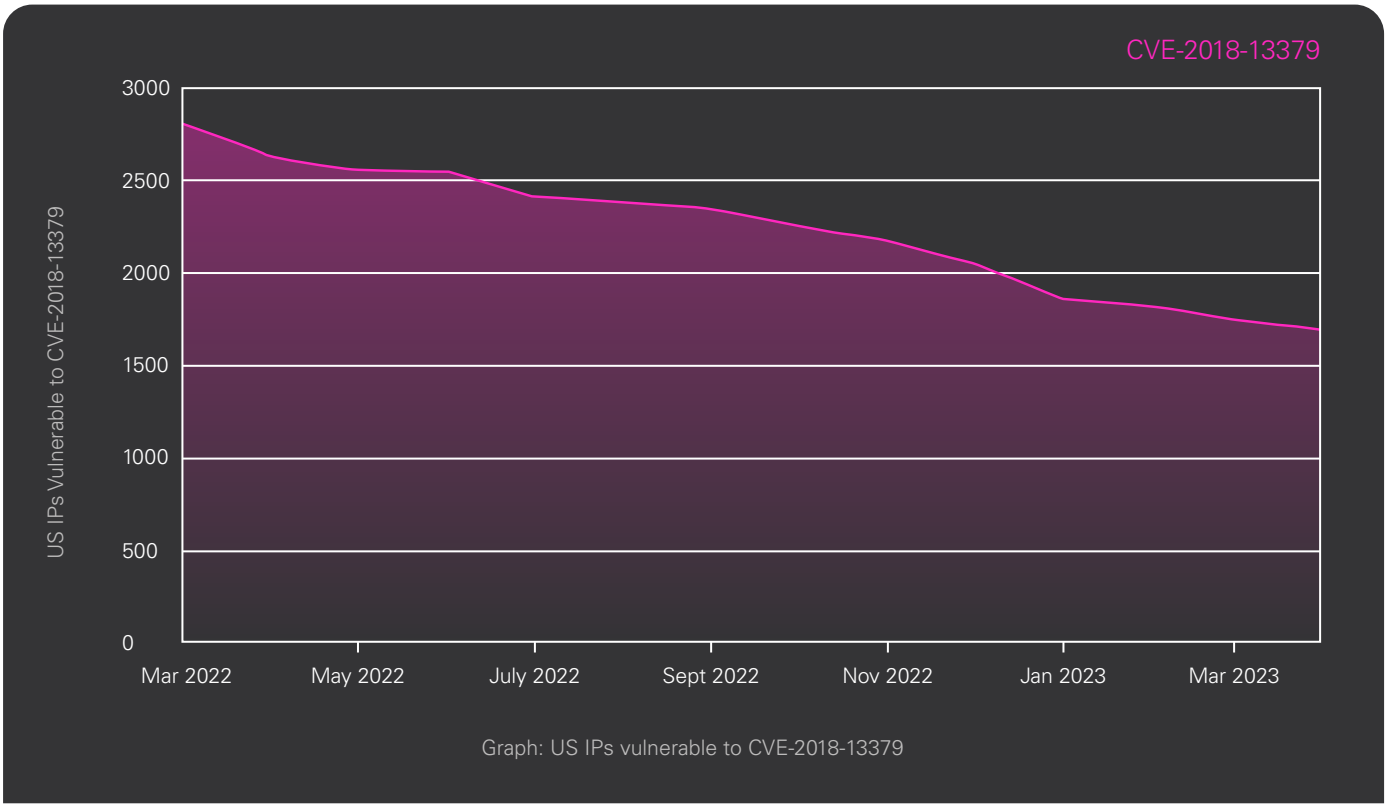
It is widely understood that a good patching cadence is critical to managing an organization's external exposure, but it can be difficult to prioritize which vulnerabilities to address. Ransomware operators are focusing on a particular subset of vulnerabilities to gain access to victims' networks through exploitation of internet-facing services. Specifically, these vulnerabilities can be exploited at-scale, affect applications and services used in enterprise networks, and provide privileged access to internal resources. For these reasons, threat-actors have targeted exploitable CVEs (Common Vulnerabilities & Exposures) in VPN devices, email applications, and file transfer and storage solutions. As seen in the recent exploitation of *GoAnywhere MFT, PaperCut* and *MOVEit* products, the Cl0p Ransomware group successfully compromised dozens of companies by developing new exploits targeting specific products, benefiting from fast, at-scale exploitation and lack of available vendor patches.

_Cont. next page

However, in this ecosystem, zero-day development is a rare occurrence, and the vast majority of ransomware compromises are still the result of initial access having been obtained through the exploitation of an older, well-known, vulnerability. Therefore, ransomware operators and Initial Access Brokers (IABs) are benefiting from freely available exploit code and a slow patching cadence.

The following are examples of older vulnerabilities still resulting in successful ransomware initial access, and subsequent network compromise:

CVE-2018-13379 is a Path Traversal vulnerability in FortiGate SSL-VPN that can allow an unauthenticated attacker to download system files via specially crafted HTTP requests. A proof of concept (PoC) has been widely available, and complexity of exploitation is trivial. Multiple Ransomware groups and IABs continue to exploit this vulnerability, including LockBit operators . Threat actors exploit CVE-2018-13379 to launch a directory-traversal attack and access the SSL VPN web session file that contains usernames and passwords in cleartext, allowing the attacker to connect remotely and establish a foothold on the network. Attackers can then also use these credentials to move laterally.



Graph: US IPs vulnerable to CVE-2018-13379

Although disclosed five years ago, this vulnerability is still widely sought after and is one of the primary methods of initial access for some well-established brokers. This is also visible in the number of malicious IPs performing daily scans and seeking vulnerable targets . Surprisingly, as shown in the graph above, remediation has been very slow, with less than 1,500 vulnerable US servers having been patched over a one-year period.

[1] "LockBit." Trend Micro Research, 8 Feb. 2022, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit.

CVE-2019-19781 is an Arbitrary File Reading vulnerability affecting Citrix Gateways and Citrix ADC (Application Delivery Controller) that can allow remote, unauthenticated attackers to perform arbitrary code execution, resulting in VPN access to an organization's network. In September 2020, a DoppelPaymer ransomware attack on the University Hospital in Dusseldorf caused an IT system failure that resulted in the death of a patient. The incident is believed to have been the first casualty reported as a direct consequence of a ransomware attack. The attackers exploited the Citrix vulnerability to gain access to the hospital's network.

When first released in December 2021, **CVE-2021-44228** (also known as "Log4Shell"), was described as one of the most severe vulnerabilities ever discovered. The vulnerability affected the Log4j2 library, a component embedded in thousands of commonly used software products and applications, including enterprise security solutions. LockBit and Black Cat/AlphaV have exploited this vulnerability for ransomware attacks, and the now inactive Conti group, was the first eCrime group to use the Log4Shell vulnerabilities as a full attack-chain. By using the now widely available PoC, attackers can achieve remote code execution on vulnerable systems.

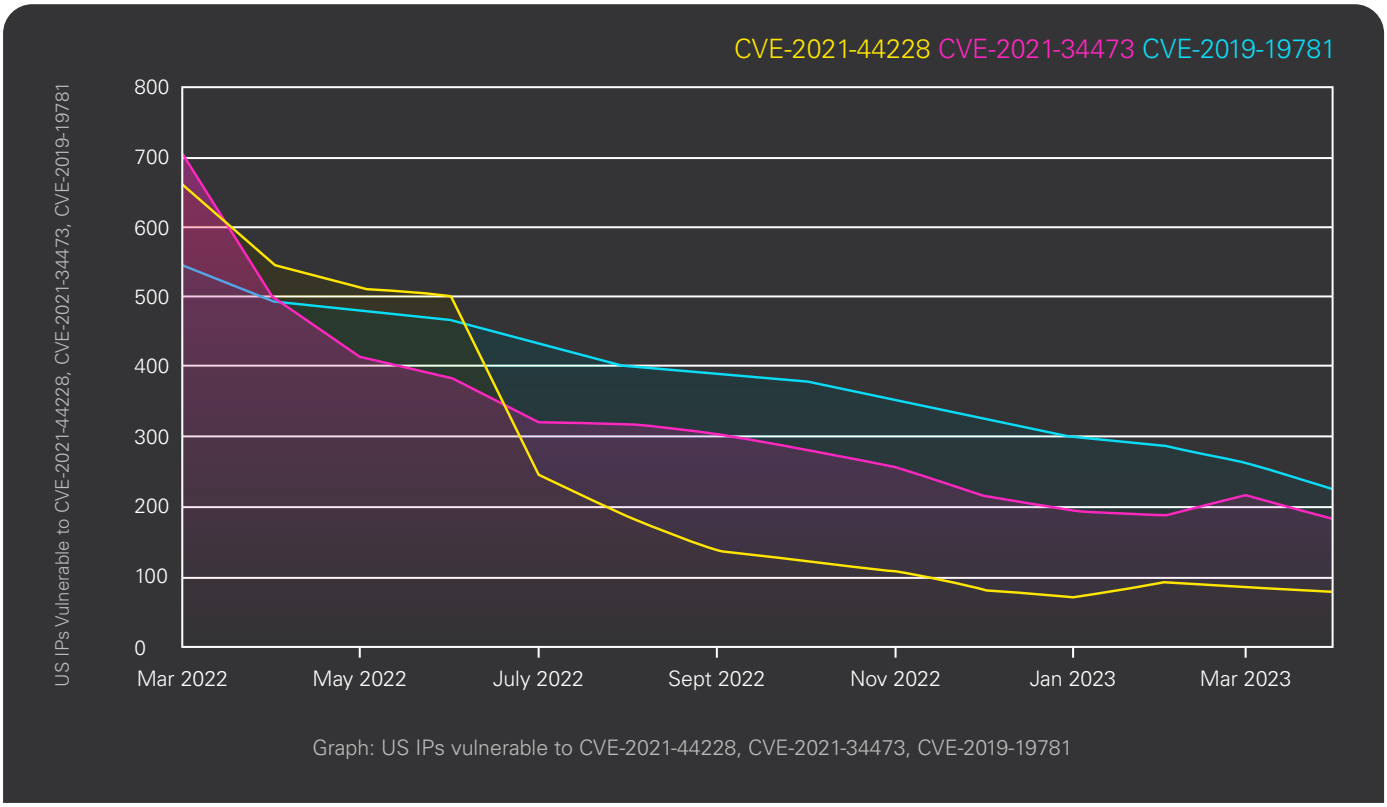
CVE-2021-34473 is the first vulnerability exploited in the chained attack dubbed "ProxyShell". Initially released in April 2021, the exploit targets Microsoft Exchange on-prem servers, and leverages CVE-2021-34473, CVE-2021-34523 and CVE-2021-31207 to allow an unauthenticated remote attacker to execute arbitrary code on vulnerable targets. Hive affiliates frequently bought access from IABs that exploited ProxyShell vulnerabilities in Microsoft Exchange servers as an initial foothold into the victim's network. Hive Ransomware, and affiliated groups, have extorted over $100 million from over 1,500 companies worldwide.

[2]Carlos E. Viera. "Fortinet FortiOS 5.6.3 – 5.6.7 / FortiOS 6.0.0 – 6.0.4 – Credentials Disclosure (Metasploit)." 19 Aug. 2019, https://viz.greynoise.io/tag/fortios-info-disclosure-attempt?days=30

[3]Lawrence Abrams. "Ransomware attack at German hospital leads to death of patient." Bleeping Computer, 17 Sept. 2020, https://www.bleepingcomputer.com/news/security/ransomware-attack-at-german-hospital-leads-to-death-of-patient/

[4]Caitlin Caimpanu. "Conti ransomware group adopts Log4Shell exploit." The Record., 16 Dec. 2021 https://therecord.media/conti-ransomware-group-adopts-log4shell-exploit

---



Graph: US IPs vulnerable to CVE-2021-44228, CVE-2021-34473, CVE-2019-19781

As observed in the graph above, **CVE-2019-19781, CVE-2021-44228** and **CVE-2021-34473** show a recognizable pattern, even after several years, hundreds of US companies remain vulnerable. The wide availability of vulnerable targets and access to free exploitation code makes these vulnerabilities a preferred method for initial access brokers to gain a foothold into corporate networks, and later sell it to ransomware operators to execute the attack. The continued probing for internet-facing vulnerable systems captured by honeypots, coupled with incident response investigations' data tracing the RPOC (Root Point of Compromise) to devices exposed to this group of vulnerabilities, highlights the direct risk associated with current exposure to these CVEs, and the need to address the overall resistance in patching.

Why Has Patching of these Vulnerabilities Been Slow?

There are many reasons why systems remain unpatched, including expired service contracts, lack of system knowledge, misconfigured patching cadence, single point of failure, or simple inability to take a system off-line due to its critical role in business continuity.

Two of the vulnerabilities discussed affect VPN and Gateway devices and they provide remote access to network resources, a critical service that requires 100% up-time. Fortinet's CVE-2018-13379, is a 5-year-old vulnerability. Based on the age of the product, it indicates the remaining vulnerable devices run a higher risk of software installation errors, reboot issues and limited support availability if reaching the End-of-Life cycle. Additionally, lack of consistent, periodic software updates can result in an extensive update path that often involves several patches to reach current software versions. In addition, hardware component failure can impact older devices, as the majority of security updates require a system restart, making them vulnerable to hardware component failure during a restart cycle.

_Cont. next page

Limited resources might indicate the absence of a backup plan if a critical service is down. As a result, organizations might avoid patching older systems and instead replace devices with newer hardware, which requires planning, and budgeting, increasing the time of exposure for vulnerable, unpatched systems.

For Microsoft Exchange, patching may not be as simple as installing the latest update. The Cumulative Update (CU) model released for Exchange 2013, 2016 and 2019, introduced a change in the update process. CU releases are similar to full upgrades, as they include multiple patches. However, as Security Updates (SU) are released monthly to address newly discovered vulnerabilities for the latest CUs, systems with older CU versions could remain vulnerable to new threats, as new SU releases may not be compatible. Due to the current amount of vulnerable and unsupported Exchange versions, Microsoft is releasing a new Exchange Online security feature that will report vulnerable or unpatched servers to the administrator, throttle email from the Exchange server, and eventually block emails from vulnerable or unpatched servers.

Patching Guidance and Best Practice

Set up an effective patch cadence and vulnerability management program to maintain the security of your organization's network. This will require the implementation of effective tools, efficient monitoring, and a thorough understanding of your company's network. It is critical to:

- Perform asset discovery by leveraging an asset management tool or leverage existing software like Active Directory, where systems are "domain-joined" and assigned to a group.
- Adopt a centralized update management tool or, for Windows environments, leverage native tools like WSUS.
- Ensure effective backups or restoration points are in place prior to rolling out updates.
- Deploy a test environment, or leverage available IT systems to test patch-deployment in a controlled setting prior to a mass rollout.
- Use patch automation whenever possible. Leverage built in features to facilitate the update process and schedule updates directly from a device interface.
- Validating a successful patch installation is critical. Leverage reporting tools to monitor the update deployment success rate. Remediate devices with failed installations.
- Leverage a vulnerability management tool like Qualys VMDR that is enriched by Threat-Intelligence to analyze the scope of impact and inform prioritization.
- Don't rely on mitigating controls as a substitute for vulnerability patching. Developments in exploitation can render an initial mitigation obsolete.

_Cont. next page

- Leverage different resources to help detect exposures when needed, including software solutions developed by the security community and adopted by CISA and other governmental entities.

- Never assume threat actors have stopped targeting a vulnerability just because the news isn't covering it anymore. Be cognizant of older vulnerabilities when introducing new software to your environment.

- In Microsoft Exchange environments: To properly manage patching, it's important to understand the difference between Cumulative Updates and Security Updates.

    - To avoid running vulnerable Exchange versions, update to the latest CU release and ensure you install additional SUs.
    - If leveraging WSUS (or similar tool) for patch management, ensure you are configured to receive security updates for your current Exchange build. Once the correct updates have been pulled, verify your deployment tasks are functioning as scheduled.
    - Ensure Exchange servers used for cloud management in hybrid environments are part of the patch cycle.

There is no guarantee that an organization is completely protected from ransomware, but at CPLG, we provide insurance, ongoing monitoring, and support throughout the life of your policy. You also get direct access to our CTI team, weekly updates on current threats, on-demand support for general cybersecurity questions, network infrastructure and security vendors. Many of these benefits can be found online and also in your policyholder portal, **cyberNET®,** which includes complimentary cyber online awareness training, phishing training and simulations, as well as sample procedures and policies to bolster your cybersecurity.

Visit us at *tmhcc.com/cyber* for more information.

TOKIO MARINE HCC

[5]The Exchange Team. Throttling and Blocking Email from Persistently Vulnerable Exchange Servicer to Exchange Online." Microsoft, 8 May 2023, https://techcommunity.microsoft.com/t5/exchange-team-blog/throttling-and-blocking-email-from-persistently-vulnerable/ba-p/3815328