CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** October 15th - October 30th
Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 21

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
PHP2Shell	Government, Public, Healthcare, Finance, and all other web facing industries.	On October 20th two RCE vulnerabilities were discovered that affect all PHP installations that serve web requests including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed. Both vulnerabilities, RCE via OOM corruption and RCE via stale global state can be exploited using crafted requests.	CISA and PHP recommend patching systems to version 8.5.12, 8.4.27, 8.3.36, or 8.2.35. For systems that cannot update to the latest version, PHP recommends hardcoding specific settings
Tailscale SSH flaw allows for privilege escalation	Infrastructure, IT	Tailworm is a group of 11 vulnerabilities discovered in Tailscale SSH that allow rapid lateral movement by utilizing device IDs and network policies without needing to obtain account names or passwords. Exploiting this requires an attacker to already control one device.	Tailscale patched Tailworm in v1.1044 and they recommend updating effected devices to that version. For systems that cannot be patched, risks can be mitigated by reviewing port forwarding, SSH rules, and app connector permissions.
Plex2Shell vulnerability chain exploitation	Government, Public, Healthcare, Finance, and industries requiring databases.	Attackers can gain unauthorized access and remotely execute code on Plex Media Server deployments by executing a chain of four vulnerabilities . Fixes were released August 3rd, but over 36,000 internet-exposed servers remained vulnerable in September.	Update to at least version 1.43.3.10861 as all prior versions are compromised. Verify the installed version and run forensic reviews on internet-facing systems for signs of compromise.

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
SafePay ransomware group	Infrastructure, Technology, Healthcare	The SafePay ransomware group targets businesses and critical infrastructure across North and South America, Europe and Australia. They gain entry by guessing passwords, exploiting vulnerabilities, and using phishing tactics. Once in the system, they use legitimate tools to move through the system, exfiltrate valuable files and then deploy ransomware.	Keep operating systems, software, and firmware up to date to avoid vulnerabilities, ensure all accounts have passwords that are strong and unique, and maintain offline backups of the system.
Lazarus (North vs South Korea)	Construction, Software, Wire-Communication	A North Korean hacker group targeting South Korean industries spanning construction, software, and wire-communication equipment manufacturing. The group targets individuals with spear-phishing emails that use links to tailored sites and then exploits vulnerabilities in mandatory financial security software to inject shellcode and install malware.	South Korean users should avoid clicking any links sent in emails from unknown sources and always verify that an email came from a legitimate source that they trust.

Important Government and ISAC Alerts

- **CISA ICS Advisories:** Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP- The additional GNU/Linux subsystem in firmware version V3.1.7 has had 428 vulnerabilities identified. Siemens recommends specific mitigations for products until fixes are available.
- **CISA ICS Medical Advisory:** InterSystems Corporation InterSystems IRIS for Health- TLS/SSL encryption is turned off by default, which allows attackers to read cleartext transmissions of sensitive data and use that information to log into devices.

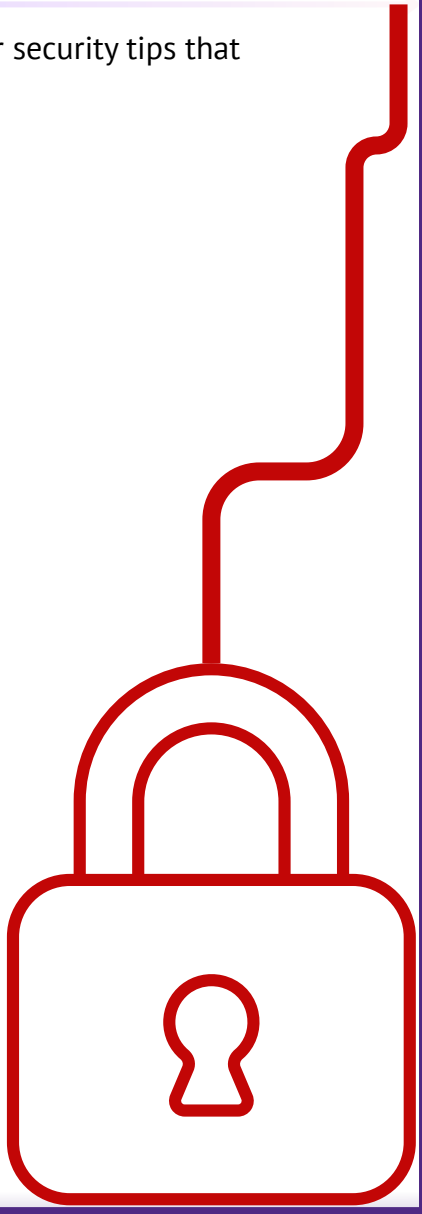
Security Awareness Theme

October Focus: Cybersecurity Awareness Month

For Cyber Security Month, the Sentinel will include a short list of general cyber security tips that can be applied to both industry and personal usage.

Cyber Security Month 5 Tips

- Passwords don't always need to be complicated strings of random characters. A long passphrase can be even stronger, and is much more memorable.
- Passwords aren't always enough to protect an account from attackers; enable multi-factor authentication on accounts, especially highly critical accounts such as banking and email.
- When receiving an email, text, or other form of communication that seems out of the normal, look for things such as calls to action, bad domains or unknown numbers, and broken grammar for possible indications of a phishing attack.
- When sharing information on social media, think of who all could see it. If your account is set to public, think if the information you're sharing could possibly be used against you.
- Public networks can have attackers who may intercept your connection and steal your information. Avoid accessing banking apps, or other applications with sensitive information, without using a VPN.



Sector-Specific Highlights

- **Healthcare: Quest Diagnostics confirms patient personal and health data breach**- Quest announced that an unspecified number of patients' records had been breached by an attack targeting its Quanum lab testing system. Over half a million clinicians across North America rely on Quanum for housing the records of over six million patients. healthcare data anonymization, as was fined $7.8 million due to the severity of the infraction.
- **Prevention Tips:** The company is still investigating what kinds of personal information was taken, but patients and clinicians should be aware of phishing emails and avoid reusing their Quanum passwords.

- **Utilities/Industrial: Sony ISP subsidiary breach exposes 2.5 million customer records-** An unauthorized party was able to obtain a total of 2,585,481 customer records from Sony Network Communications, which contains information such as full names, phone numbers, email addresses, user IDs, and birth dates, with an additional 54,401 email addresses exposed along with passwords.
- **Prevention Tips:** Sony and other affected companies advised customers to change passwords and warned of phishing emails and fake websites pretending to be the companies.

- **Education: Frontline Education data breach**- A vulnerability was discovered in a third-party software used by Frontline Education that led to unauthorized access to their system. This access led to the compromise of social security numbers, dates of birth, driver's license numbers, passport numbers, government IDs, Medicaid IDs, and student IDs.
- **Prevention Tips:** Potentially affected individuals have been notified. If affected, it is recommended to remain vigilant against threats of identity theft or fraud. If you suspect you are a victim, contact your local police.

- **Public Safety/Financial: Citizens Bank data breach-** Citizens Bank has reported a data breach where names, social security numbers, date of births, phone numbers, and email addresses were exposed. They reported that they found no evidence that the data was examined or used maliciously, and they haven't reported how the breach happened or how many people were affected.
- **Prevention Tips:** It is recommended to remain vigilant against threats of identity theft, fraud, or phishing attempts. If you suspect you are a victim of identity theft or fraud, contact your local police.

Recommended Tools and Federal Resources

- Google Safe Browsing – A toolset used by many major products that identifies known phishing and malware on the internet and alerts users and website owners of potential harm.
- Dastardly, from Burp Suite - A web application security scanner that runs CI-driven scans on CI/CD platforms like TeamCity, Jenkins, GitHub Actions, and Platform Independent, viewing the application like an outside attacker.
- Weak Password Test - Tests passwords in the Microsoft Active Directory for ten different types of password weaknesses and generates a report of users with weak passwords and why they failed.

Emerging Trends to Watch

- **Threat actors abuse Microsoft Teams external chat for access:** A social engineering pattern has emerged where threat actors are using Microsoft Teams external chats to impersonate IT support and gain remote access to a machine with Quick Assist, AnyDesk, or ScreenConnect. Once they gain access, they install malware on the system. These impersonation attacks usually happen during or after a flood of scam messages. To prevent this attack, have an admin disable external chats for the organization. If external messages are required, an admin can create an allow-list to only let specific domains into external chats or block any unmanaged or trial-only teams accounts.
- Fake AI attacks spread across US: Attackers are stealing credentials and distributing malware by impersonating AI products. These attackers create fake download and login pages based on legitimate AI websites and then use search ads, email invites, and other tactics to get people on to the website. Once the user tries to login or download the tool, the attacker has their credentials or can make use of whatever malware the website installed. To prevent this, ensure that you are on the real website for the AI you are trying to use before trying to login or download anything. Check for any changes to the url or layout of the website.
- Critical Brotli vulnerability identified: A vulnerability in Brotli C decoder, known as Broccoli2Shell, can cause the library to write out-of-bounds when given specially crafted compressed data. This can lead to memory disclosure, application crashes, or arbitrary code execution. This affects Google Brotli, Python Brotli, Python brotlicffi, Node.js, Bun, Envoy Proxy, Istio, and andybalholm/brotli. This vulnerability is also known as Node2Shell and HTTP2Shell. Update affected systems to the recommended patch version. Identify any potentially vulnerable workloads and applications and ensure they are patched before redeploying them.