CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** February 2nd, 2025 - February 13th, 2026
Distribution: Public Sector Partners, Local Governments, IT Departments *Volume 2 Issue 3*

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Autodesk 3ds Max File Vulnerability	Media & Entertainment, Creative Services	A vulnerability in Autodesk 3ds Max allows a specially crafted image file to cause the application to crash or run malicious code when the file is opened. The issue stems from a Stack-Based Buffer Overflow vulnerability.	Install the latest security update for Autodesk 3ds Max (mitigated in 2026.3.2) as soon as possible and avoid opening untrusted GIF files from unknown sources.
BeyondTrust Remote Support RCE	Finance, Managed Service Providers	A pre-authentication Remote Code Execution (RCE) vulnerability allows an attacker to send specially crafted network requests to the target system. This request triggers a flaw in the system's command execution handler allowing for arbitrary code execution.	Update BeyondTrust Remote Support to version 25.3.2 (or later), and Privileged Remote Access to version 24.3.5 (or later). In the meantime, restrict access to the BeyondTrust admin interfaces to a strictly defined list of known safe IP addresses.
Open62541 Library DoS & RCE	Manufacturing	An out-of-bounds write flaw has been affecting the Open62541, a popular open-source implementation of Open Platform Communications Unified Architecture (OPC UA). This allows attacker to send network packets to a device, leading to a Denial of Service or Remote Code Execution.	Ensure all systems running Open62541 are promptly updated to version 1.5-rc2 (or later).
Vzaar Media Cross Site Scripting	Media Organizations, Digital Publishers	Attacker can engage in Reflected Cross-Site Scripting thanks to a vulnerability regarding insufficient input sanitization.	Immediately update the Bzaar Media Management plugin to version 1.3 or newer. Implement a strict Content Security Policy (CSP) header on your media site to prevent the execution of unauthorized inline scripts.
APT29 Threat Actors	General	APT29 is a Russia-linked, state-sponsored cyber-espionage group that primarily targets government agencies, diplomatic organizations, and public-sector entities to collect sensitive information.	Secure accounts by enforcing MFA for email and remote access, auditing permissions regularly, and monitoring for unusual activity.

CERIAC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** Hitachi Energy FOX61x Products *Vulnerabilities affecting Hitachi Energy FOX61x products that could allow unauthorized access or disruption of operations if exploited.*
- **CISA ICS Medical Advisory:** WHILL Model C2 Electric Wheelchairs and Model F Power Chairs *A critical flaw could allow an attacker within Bluetooth range to remotely connect to and control WHILL Model C2 and Model F power chairs without authentication.*

Security Awareness Theme

February Focus: Password Security

Passwords are the backbone of our digital security; from the way we unlock our phones to the way we log in to all our online accounts. Over 68% of successful cyberattacks still originate from human error or credential misuse. Billions of stolen username-password pairs are traded on the dark web. If you reuse a password from a personal shopping site for your email, an attacker can automate attempts to log in to your professional accounts in seconds.

Prioritize Length over Complexity

- Short passwords can be cracked relatively fast, regardless of complexity.
- Instead, try implementing **Passphrases** for additional security.
- Example:
  - Old: P4ssw0rd67
  - New: iLoveMyD0gs4ever&theyLoveMe!

Make Multi-Factor Authentication Mandatory

- Create alternative ways to log in to your accounts.
- This way, attackers need more than just a password.
- If one factor is compromised, you can reset it.
  - Just use another form to verify your identity!
- Use MFA on all important online accounts.

Sector-Specific Highlights

- **Healthcare:** GNU InetUtils Authentication Bypass - An 11-year-old flaw in the "telnetd" daemon was recently discovered being actively weaponized. It allows unauthenticated attackers to bypass authentication entirely and gain a root shell by injecting malicious environment variables during the login handshake. ***Prevention Tips:*** *Disable telnetd across all systems and use SSH if possible.*

- **Utilities/Industrial:** FreeRDP Heap Buffer Overflow - The People's Republic of China has positioned malicious software in critical infrastructure devices across the United States within the industrial sector. This software is designed to "brick" or completely disable the infected device. ***Prevention Tips:*** *Upgrade all FreeRDP-based clients to version 3.21.0 or higher.*

- **Education:** Harvard University Data Breach – On February 4th, 2026, the ShinyHunters syndicate breached the fundraising and donor relations database of Harvard University. The breach resulted in the exfiltration of approximately 115,000 record with sensitive data. ***Prevention Tips:*** *Incorporate Mutli-Factor Authentication and use Identity Protection (i.e., keep a whitelist of known IP addresses).*

- **Public Safety/Financial:** Microsoft Office Security Bypass - This vulnerability centers on how Office handles Object Linking and Embedding (OLE) objects. It allows an attacker to force the victim's computer to fetch and execute a remote payload via the WebDAV protocol. ***Prevention Tips:*** *This vulnerability was patched out on January 28, 2026, in their "Patch Tuesday" cycle. All users are advised to update their systems as soon as possible. Alternatively, you can block outbound WebDAV protocol traffic at your network firewall.*

Recommended Tools and Federal Resources

- CISA KEV Catalog – Provides a curated list of vulnerabilities that are confirmed to be actively exploited in the wild to help defenders prioritize patching.
- CISA Cyber Hygiene Services – Provides no-cost assistance such as scanning and assessments to help organizations reduce their exposure to cyber threats.
- NIST Cybersecurity Framework – A voluntary framework to help organizations manage and reduce cybersecurity risk.

Emerging Trends to Watch

- Abuse of Valid Accounts and identity Misconfigurations– Attackers are increasingly abusing valid accounts and identity misconfigurations to gain access, often using stolen credentials, excessive permissions, or missing multi-factor authentication in cloud environments. ***Prevention Tips:*** *Use Mutli-Factor Authentication, limit user permissions, and monitor login activity.*

- Supply Chain Malware via Third-Party Software Updates – Attackers are compromising trusted software updates to deliver malware to many organizations at once. ***Prevention Tips:*** *Use trusted updates only, restrict access to update systems, and monitor systems for unusual activity.*

- *Generative AI Targeted Phishing Campaigns* - Attackers are using generative AI and automation tools to create highly convincing phishing emails and messages that are harder for users and traditional filters to detect. These campaigns often mimic trusted entities and can lead to credential theft or deployment of malware. ***Prevention Tips:*** *Train users to recognize unusual or unexpected requests, implement advanced email filtering and authentication, and use multi-factor authentication to reduce the impact of compromised credentials.*