

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** September 5th - September 18th

Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 18

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Cisco ISE Authentication Bypass Vulnerability	Education, Finance, Government, Healthcare, Manufacturing	Cisco warns of a maximum-severity security flaw impacting Identity Services Engine due to insufficient authentication control on an API endpoint. The flaw allows remote attackers to bypass authentication by sending a crafted request to an affected API endpoint to bypass the web-based management interface and obtain root privileges.	The vulnerability has been patched in Cisco ISE versions 3.1 Patch 12, 3.2 Patch 11, 3.3 Patch 12, 3.4 Patch 7, and 3.5 Patch 4. It is highly recommended to update ISE to these versions.
Improper Limitation of a Pathname to a Restricted Directory in GitLab	Education, Finance, Retail, Science & Research, Technology, Utilities	GitLab released patches for multiple critical security flaws, including a maximum-severity path traversal vulnerability that allowed unauthorized users to read arbitrary files from the GitLab server under certain conditions due to improper path confinement and missing authentication enforcement in the repository commits API.	The vulnerability has been patched in GitLab versions 19.1.8, 19.2.6, and 19.3.2 among other highly critical security flaws.
LiteSpeed Enterprise flaw allows accounts to gain root access on shared servers	IT Services	A critical vulnerability has been identified in LiteSpeed Web Server Enterprise that could allow a malicious user to gain root-level access on shared servers. This vulnerability can also bypass account isolation controls, which allows an attacker to escape their restricted environment and gain access to other hosted websites and the server itself.	Any version prior to 6.3.7 is affected by the vulnerability, so it is recommended to update the LiteSpeed Web Server Enterprise to 6.3.7 if that has not already been done.

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Red Heron	Defense, Aerospace, Telecommunica tions, Energy, Elections, Government	Red Heron is a suspected Chinese threat actor that has been rapidly exploiting a recently disclosed security vulnerability in Gitea to compromise internet-facing instances. Red Heron achieves initial access by using automated tooling to exploit an RCE vulnerability in internet-facing Gitea servers. Once inside, they deploy tooling to hide processes, connections, and files, while maintaining persistence. From there, they move laterally to exfiltrate codebases and credentials.	The vulnerability that Red Heron exploits affects versions 1.17 through 1.27.0 of Gitea. It is recommended to update to version 1.27.1, disable open registration on instances where it is not required, restrict the diffpatch API route where not used, and not exposing Fitea to the internet where a VPN or reverse proxy with authentication is practical.
Hacking Cat	Russian Enterprise and Infrastructure	A pro-Ukrainian hacktivist group targeting Russian organizations with the use of remote access trojans and ransomware. The group has also been observed collaborating with other hacktivist groups such as Cyber Anarchy Squad and the Ukrainian Cyber Alliance to share tools and coordinate attacks.	Hacking cat uses CVE-2021-26855 and CVE-2026-42897 to gain initial access. Both are vulnerabilities on Microsoft Exchange servers, and both are patched.



Important Government and ISAC Alerts

-  **CISA ICS Advisories: [AVEVA Pipeline Integrity Monitor](#)**- An attacker can exploit a hard-coded cryptographic key, a broken or risky cryptographic algorithm, missing authorization, or improper neutralization of input during web page generation to disclose information, brute-force hashes, or run arbitrary code in a browser session.
- **CISA ICS Medical Advisory: [NextGen Healthcare Mirth Connect](#)**- An attacker can exploit improper neutralization of special elements used in an SQL command or improper restriction of XML external entity reference to exfiltrate data or cause a denial-of-service condition.



Security Awareness Theme

August Focus: Rogue AI Agents

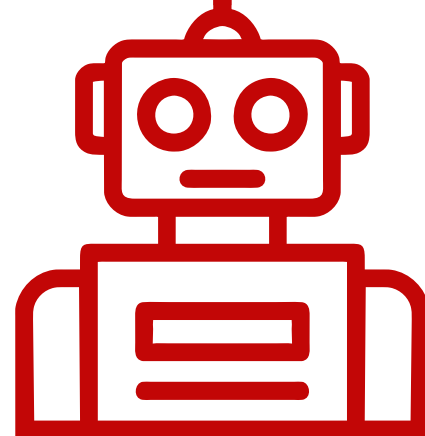
As AI models become more powerful, and research projects become more intense, the possibility of rogue AI agents becomes more of a reality. An AI agent is considered rogue when it judges that an action, even if it violates its original scope or rules, progresses it towards its goal and performs that action anyways; agents going rogue can possibly cause harm to the testing environment, or the agent may breach the testing environment entirely. A recent example is the breach of OpenAI agents and a subsequent intrusion into Hugging Face systems.

Now that rogue agents are not just a fear and have become a reality, large language model providers such as OpenAI and Anthropic face ridicule from multiple governments, claiming that the lack of control could provide a large danger to financial sectors and general business. AI providers must now implement kill switches and other more extreme security measures to regain the trust of the overall public.



When running strong AI models, make sure to

- Provide strong boundaries, even if the research is based on reduced safeguards in models
- Make sure that access to the wider internet is impossible for models, even if they were to breach the testing environment
- Properly keep track of agent goal alignments with alerts and surveillance
- Avoid giving tasks to AI agents where the likelihood of going rogue would be high





Sector-Specific Highlights

-  **Healthcare: McKesson Cyberattack Steals 6.4 Million Email Addresses**- A cyberattack on McKesson, a major American healthcare corporation, has resulted in the unauthorized access and exfiltration of sensitive patient, staff, and marketing campaign information, including 6.4 million unique email addresses.
- Prevention Tips:** McKesson is reportedly implementing additional cybersecurity measures to prevent similar breaches from occurring in the future and is working with third-party cybersecurity experts to monitor its systems and the internet for activity related to the event.
-  **Utilities/Industrial: Dispel Launches Cybersecurity Program for Small U.S. Water & Electric Utilities**- Dispel announced their Community Power & Water Program to provide small utilities (of 1-3 staff members) with secure remote access solutions against risks like exposed PLCs and remote access. Dispel seeks to address numerous recent attacks on critical U.S. infrastructure exploiting internet-exposed PLCs, including over 30 Minnesota municipal water utilities reporting cyberattacks within 48 hours in late July 2026.
- Prevention Tips:** CISA advisory AA26-097A lists removing PLCs from internet-facing exposure as the top control for reducing cyberattack risk.
-  **Education: Springfield, Massachusetts schools reveal hackers stole teacher data**- Schools in Springfield, Massachusetts were forced to close for a week after their systems became infected with ransomware. The hackers have since posted the stolen data online, but the systems are being restored slowly and steadily.
- Prevention Tips:** The exact cause of the ransomware appearing on the system has not been released, so for now the best prevention advice that can be provided is to be careful about the links you click and the files you download.
-  **Public Safety/Financial: Online shops in danger after Magento zero-day exploit**- A vulnerability has been discovered in Magento/Adobe Commerce, a major e-commerce platform, that could allow an attacker to execute arbitrary code without any user interaction or privileges. Attackers can inject malicious PHP code into the template system, which will run when Magento tries to render the template.
- Prevention Tips:** It is recommended to install the most recent patch released by Adobe to resolve this vulnerability.



Recommended Tools and Federal Resources

- [John the Ripper Password Cracker](#) – An open-source password security auditing and password recovery tool available for many operating systems.
- [Ransomware Risk Assessment](#) - Web browser tool that assesses an organization's ability to counteract a ransomware infection and its spread, including its defenses against initial compromise, lateral movement, and data loss/exfiltration.
- [Garak](#) - An open-source tool to automate testing for vulnerabilities in AI models by generating adversarial prompts and recording the model's response.



Emerging Trends to Watch

- [Parallels Desktop flaw allows non-admins to gain root access](#): Parallels Desktop, a hypervisor for Macs, has a flaw that allows ordinary users to gain root access on the Mac running it. By manipulating the command to install a virtual machine appliance, a user can run any program as root. For Macs with an Apple silicon chip, updating to the latest version should fix the flaw. For other Macs that can't install the fixed version, the best thing to do is to limit who can log in locally until an official fix is released.
- [DeepSeek Harness flaw lets AI agents disable their own sandbox](#): A flaw in DeepSeek Harness allowed AI agents to escape their own sandbox by calling the tool's web interface on the same machine, causing its commands to run outside the sandbox without any approval. If possible, update DeepSeek Harness to version 0.1.2-rc.1. If that is not an option, stop the web interface when it is not in use and remove any tunnel, proxy, or port forward that reaches it.
- [Apache Syncope vulnerabilities allow for malicious code execution and control bypasses](#): Vulnerabilities have been disclosed that would allow an admin with sufficient permissions to perform an SQL injection attack using the Task search feature, bypass intended protections with a malicious Groovy Command, or take over JWT access-tokens. The best way to prevent this currently is to apply the principles of least privilege. Since no patch to fix these vulnerabilities has been released yet, ensure that everyone only has the minimum permissions they need to do their job.