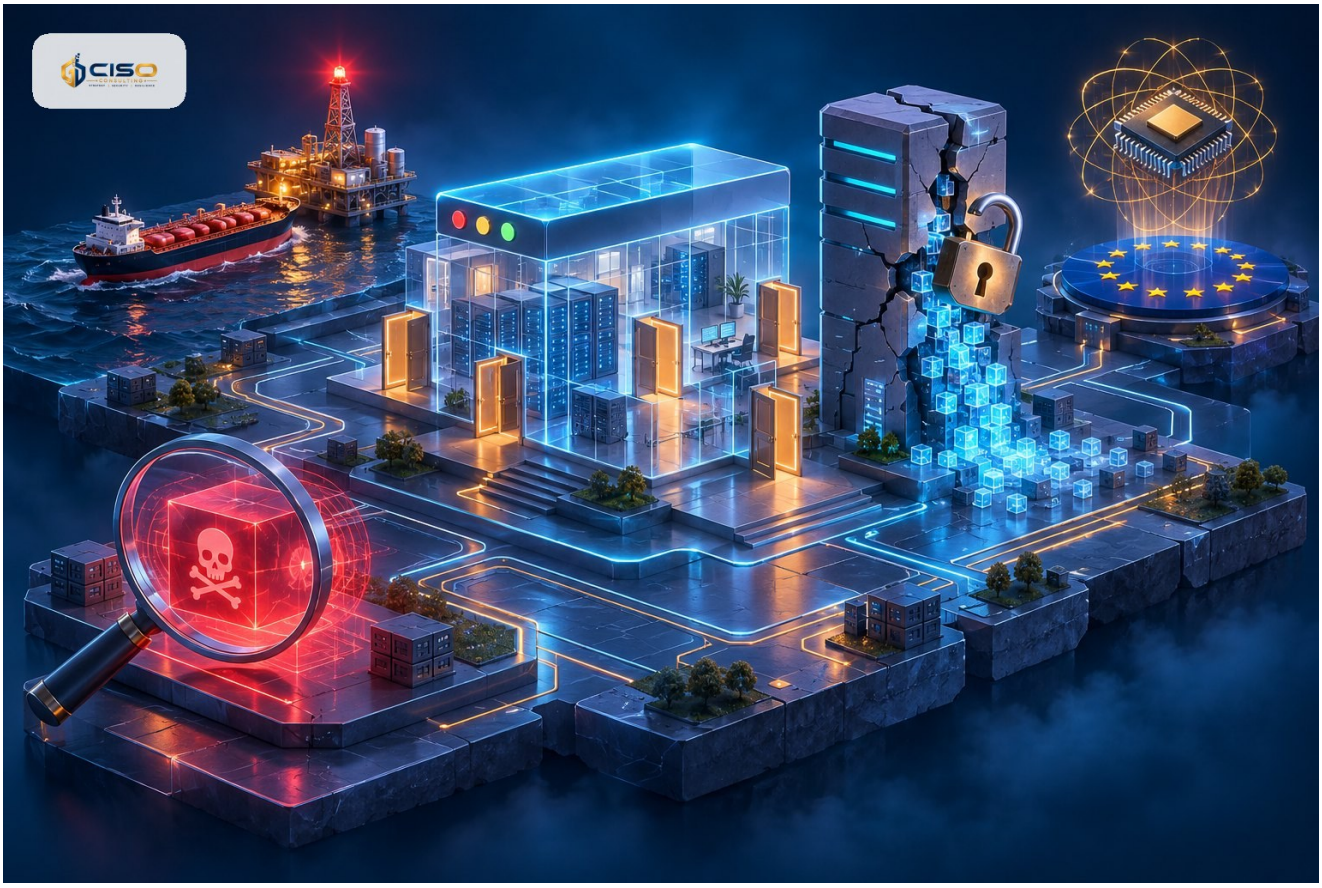
Weekly roundup: exposed AI-built sites, Radware API breach and tanker attacks



SecurityWeek's weekly roundup covers exposed ChatGPT Sites, an unprotected Radware API, AI-assisted intrusion tooling, new VirusTotal ransomware detection and the EU Quantum Act. Several items bear on access control and cryptographic planning.

- Pluto found 16,666 ChatGPT Sites, 12,830 publicly accessible, with sensitive data exposed at 27 organizations.
- Radware was reportedly breached through an internet-exposed Cloud WAF management API; customer contacts and some cloud and SFTP credentials may be affected.
- Microsoft reports state-sponsored groups and criminals using the AI-powered framework Artex, reaching privileged access and persistence within minutes.
- The EU's proposed Quantum Act includes measures to speed up post-quantum cryptography

adoption.

- SolarWinds Serv-U and several Adobe products received patches for critical flaws.

SecurityWeek's weekly roundup gathers items that may not receive standalone coverage. Several are relevant to institutions that depend on cloud services, external vendors and file-transfer tools.

Exposure through convenience and management interfaces

Researchers at Pluto identified 16,666 sites built with ChatGPT Sites, which builds and hosts web apps. Of these, 12,830 were reachable by anyone, and manual checks confirmed sensitive data exposure at 27 organizations. Sites are visible only to owners and admins by default, but owners can open them to the internet.

Separately, an internal report seen by BleepingComputer indicates that Radware was breached through an unprotected Cloud WAF management API exposed to the internet. Customer contact details and credentials for AWS, Azure and SFTP storage used by some customers may have been compromised. The company has not commented.

Faster attackers and patches

Microsoft says state-sponsored groups, including Salt Typhoon, and cybercriminals are using the AI-powered penetration testing framework Artex to find exposed secrets in public repositories, mount supply chain attacks and locate vulnerable systems. Attackers reportedly gain privileged access and persistence within minutes.

SolarWinds patched critical flaws in Serv-U, including privilege escalation and arbitrary code execution. Adobe fixed critical issues in Campaign Classic and Experience Manager, plus a medium-severity DoS flaw in InDesign.

Longer-term signals

The European Commission's proposed Quantum Act includes measures to accelerate post-quantum cryptography. VirusTotal also added ransomware detection based on observed file encryption in sandbox analysis.

The common thread is that routine exposure, not sophisticated exploitation, often opens the door. A review of what is publicly reachable is a sensible next step.

What to do now

1. Inventory AI-built and low-code sites and apps in use, and confirm none are shared publicly or hold sensitive data.
2. Ensure management APIs and consoles are not exposed to the internet; restrict them by network and

strong authentication.

3. If you use Radware Cloud WAF, watch for vendor notices and consider rotating related AWS, Azure and SFTP credentials.
4. Patch Serv-U and the affected Adobe products promptly, prioritizing internet-facing instances.
5. Scan public code repositories for exposed secrets and rotate any found.
6. Add post-quantum cryptography to your cryptographic inventory and roadmap.