

Daily Cyber Headlines

Daily Cyber
Headlines

TLP:WHITE

Alert ID :
666c4bcd

Oct 07, 2025, 05:44
AM



Today's Headlines:

Leading Story

- Redis Warns of Critical Flaw Impacting Thousands of Instances

Data Breaches & Data Leaks

- Data Breach at Doctors Imaging Group Impacts 171,000 People

Cyber Crimes & Incidents

- Suspected Chinese Cyber Spies Targeted Serbian Aviation Agency

Vulnerabilities & Exploits

- Oracle Rushes Patch for CVE-2025-61882 After Clop Exploited It in Data Theft Attacks

Trends & Reports

- XWorm Malware Resurfaces with Ransomware Module, Over 35 Plugins

Privacy, Legal & Regulatory

- [Europol Calls for Stronger Data Laws to Combat Cybercrime](#)

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
 - Americas – October 28, 2025, 12:00-01:00 PM ET
 - European – October 29, 2025, 03:00-04:00 PM CET
- [European Summit](#) – Rome, Italy – October 14-16, 2025
- [Fall Americas Summit](#) – Carlsbad, California – December 1-5, 2025

Additional Information

Leading Story

[Redis Warns of Critical Flaw Impacting Thousands of Instances](#)

Summary

- A critical RCE flaw CVE-2025-49844 affects all Redis versions due to an old Lua feature; immediate patching is advised.

Analysis & Action

A maximum-severity Remote Code Execution (RCE) vulnerability, CVE-2025-49844, dubbed RediShell, has been disclosed. The flaw has a CVSS score of 10 and affects all Redis versions.

This use-after-free flaw is present in the default-enabled Lua scripting feature. Exploitation, which requires initial authentication, allows threat actors to establish a reverse shell and gain full system access, enabling credential theft, lateral movement, or data exfiltration. The risk is amplified by Redis's widespread use across approximately 75% of cloud environments and the discovery of around 330,000 online instances, with over 60,000 not requiring authentication.

Immediate patching to fixed releases is advised, prioritizing internet-exposed instances. Further hardening of the defenses, including enabling authentication, disabling unnecessary commands, using non-root accounts, and implementing network-level access controls via firewalls and VPCs to mitigate future exploitation, is also advised.

Data Breaches & Data Leaks

[Data Breach at Doctors Imaging Group Impacts 171,000 People](#)

Summary

- A Florida radiology practice, Doctors Imaging Group, has confirmed a data breach from November 2024 that compromised highly sensitive information from over 171,000 patients.

Analysis & Action

Doctors Imaging Group has confirmed a data breach from November 2024 that exposed sensitive information from over 171,000 individuals.

The investigation revealed that threat actors gained access to the radiology practice's network and exfiltrated large amounts of data from the compromised systems. Such information included contact details, social security numbers, financial account information, medical records, and other related healthcare data. The responsible threat actors have yet to be identified.

Health-ISAC recommends that its members encrypt all stored and in-transit data, consider network segmentation, and employ network firewalls to mitigate potential data breaches.

Cyber Crimes & Incidents

[Suspected Chinese Cyber Spies Targeted Serbian Aviation Agency](#)

Summary

- Cybersecurity researchers have unveiled a recent cyber-espionage campaign by Chinese threat actors that targeted several European institutions through phishing emails and malware deployment.

Analysis & Action

StrikeReady confirmed a recent cyber-espionage campaign by Chinese threat actors that targeted several European institutions, including the Serbian government's aviation department.

The campaign leveraged phishing emails on fake European government business agendas to target institutions in Italy, Belgium, Hungary, the Netherlands, and Serbia. The email messages contained malicious links that, upon interaction, redirected users to an illegitimate Cloudflare verification page. The threat actors also leveraged various malware tools like Sogu, PlugX, and Korplug. This malware suggests a potential connection between the threat groups and the Chinese government, likely sponsoring

the cyber-espionage campaigns. It remains unclear if threat actors succeed in their campaigns and if information is exfiltrated.

Health-ISAC advises its members to educate all staff on social engineering campaigns, report suspicious activity to the appropriate department, and avoid interacting with suspicious communication as mitigation measures.

Vulnerabilities & Exploits

[Oracle Rushes Patch for CVE-2025-61882 After Clop Exploited It in Data Theft Attacks](#)

Summary

- Oracle has released a new security patch to address the actively-exploited vulnerability, CVE-2025-61882, in the ongoing campaign targeting E-Business Suite instances.

Analysis & Action

Oracle has released an emergency security patch for a critical vulnerability, CVE-2025-61882, in E-Business Suite platforms that was recently exploited by Clop ransomware.

The latest security update fixes a remotely exploitable flaw that requires no user authentication and can enable remote code execution. The patches also addressed additional potential exploits discovered during recent incident investigations. According to Mandiant, the ransomware group had exploited CVE-2025-61882 and past vulnerabilities patched in July this year in its latest, large-scale email campaign. Oracle also released a series of compromise indicators (IoCs) indicating a potential collaboration between Clop and LapSUS\$ Hunters threat groups.

Health-ISAC encourages all members to patch all vulnerable software promptly, avoid interacting with suspicious emails, and educate all staff on the ongoing campaign to mitigate potential exploits and subsequent breaches.

Trends & Reports

[XWorm Malware Resurfaces with Ransomware Module, Over 35 Plugins](#)

Summary

- Researchers have identified new variants of the temporarily discontinued malware XWorm, which now support additional functionalities and over 35 plugins for advanced malicious activity.

Analysis & Action

Threat actors have developed new XWorm remote access trojan (RAT) variants, often used in phishing campaigns, that allow for plugins and a wider range of malicious activities.

The malware, temporarily discontinued by its original developer, has been picked up by other threat actors. Commonly used for data exfiltration, the malware carries encryption, remote session, and recording capabilities. The latest versions—6.0, 6.4, and 6.5—address a previous remote code execution vulnerability and support over 35 plugins that range from information stealers to ransomware. Recent reports on the new XWorm variants also reveal new attack tactics beyond common email-based campaigns.

Health-ISAC encourages its members to deploy endpoint detection and response (EDR) tools, actively review network logs, and employ email filtering solutions as mitigation measures.

Privacy, Legal & Regulatory

[Europol Calls for Stronger Data Laws to Combat Cybercrime](#)

Summary

- The Europol's latest Annual Conference in The Hague highlighted the need for stricter cybersecurity regulations and information sharing between industries and governments to mitigate against evolving threats.

Analysis & Action

Europol has shared the latest threats and challenges within cyberspace in its Annual Cybercrime Conference, particularly highlighting the need for stricter legislation and collaboration.

Delegates from the agency noted that threat actors are increasingly developing their attack techniques, which is affecting how cybercrime investigations occur. Such evolution requires a stronger response by governing authorities and a collaborative approach by industries to mitigate existing and potential threats. Europol urged attendees to consider cross-border data sharing and cyber diplomacy with local and

federal governments. The summit also included a workshop led by the Computer Security Incident Response Teams (CSIRTs) and ENISA, emphasizing information sharing between European bodies.

Health-ISAC encourages its members to actively participate and share threat intelligence to mitigate emerging threats that target the sector.

Health-ISAC Cyber Threat Level

On September 18, 2025, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level to **Blue (Guarded)**. The Threat Level of **Blue (Guarded)** is due to threats from:

NPM Worm Impact, QR Code Phishing, Typosquatting Campaigns, Remote IT Worker Fraud, and Job Posting Scams.

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

**You must have Cyware Access to reach the Threat Advisory System document.
Contact membership@h-isac.org for access to Cyware.**

Report Source(s)

Health-ISAC

Tags

Xworm RAT, Chinese threat actors, Europol, Redis, Data Breaches, Oracle

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" [here](#).

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" [here](#).

Access the Health-ISAC Threat Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org