# Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : b73fa59a | Oct 23, 2023, 06:40 AM

**Today's Headlines:**

**Leading Story**

- Cisco Zero-Day Exploited to Implant Malicious Lua Backdoor on Thousands of Devices

**Data Breaches & Data Leaks**

- Okta Says Its Support System Was Breached Using Stolen Credentials
- North Carolina Hospital Suffers Data Breach

**Cyber Crimes & Incidents**

- Fake Corsair Job Offers on LinkedIn Push DarkGate Malware
- Ragnar Locker Ransomware Developer Arrested in France

**Vulnerabilities & Exploits**

- Critical RCE Flaws Found in SolarWinds Access Audit Solution

**Trends & Reports**

- September 2023 Healthcare Data Breach Report

**Privacy, Legal & Regulatory**

- Nothing to Report

**Cybersecurity Awareness Month**

- The Daily Cyber Headlines are being shared during the month of October at **TLP:WHITE** for Cybersecurity Awareness Month.

**Upcoming Health-ISAC Events**

- Americas Hobby Exercise - October 25, 2023. Registration is available here.
- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

**Additional Information**

**Leading Story**

Cisco Zero-Day Exploited to Implant Malicious Lua Backdoor on Thousands of Devices

**Summary**

- Cisco is warning about a new zero-day vulnerability used in an exploit chain.

**Analysis & Action**

Cisco is warning about a new vulnerability actively exploited in zero-day attacks to deploy lua-based implants in a malicious operation.

The vulnerability, tracked as CVE-2023-20273, is a privilege escalation bug and is affecting web UI features. The vulnerability is used in an exploit chain alongside the CVE-2023-20198 vulnerability, which was reported last week.

During the identified operation, the attackers first used CVE-2023-20198 to gain initial access and to create a local user account, and afterward used CVE-2023-20273 to elevate the privileges of the said local user to root and write the implant to the file system.

Cisco has released updates addressing the two exploited vulnerabilities. More information can be accessed here.

Health-ISAC has previously sent targeted alerts to members who were affected by CVE-2023-20198.

**Data Breaches & Data Leaks**

Okta Says Its Support System Was Breached Using Stolen Credentials

**Summary**

- Okta suffered a data breach, compromising customer cookies and session tokens.

**Analysis & Action**

Identity Access Management (IAM) firm Okta suffered a data breach when attackers allegedly breached its support management system using stolen credentials and were able to access files containing customer cookies and session IDs.

According to Okta, the support system breached is separate from the production version of Okta, therefore ensuring that production Okta functions have been unaffected. However, this means that session IDs and cookies associated with support cases may be at risk of publicization. Cookies and session ID information are typically collected by info-stealing malware and sold on log markets.

Members who have recently had to contact Okta support for any reason should expire their cookies and encrypt the information stored within them.

[North Carolina Hospital Suffers Data Breach]

**Summary**

- Cape Fear Valley Health disclosed a breach as a result of a supply chain compromise during the MOVEit incident.

**Analysis & Action**

Cape Fear Valley Health, a care delivery organization from North Carolina, United States, disclosed a data breach.

The data breach affected close to 2,000 patients, and breached information included patients' names, addresses, dates of birth, and medical diagnoses. The breach was reportedly a consequence of a vendor compromise.

Westat, a software used for clinical trials and disease surveillance, among other things, was compromised in the MOVEit incident in May, enabling the threat actors' access to the networks of its clients as well.

The MOVEit incident compromised many healthcare institutions via their healthcare-related software vendors, highlighting the dangers of supply chain compromise attacks. We urge members to always have a current backup of their data, as well as to follow stringent vendor risk management processes.

## Cyber Crimes & Incidents

[Fake Corsair Job Offers on LinkedIn Push DarkGate Malware]

**Summary**

- A Vietnamese threat actor group uses fake LinkedIn posts and direct messages to lure victims into downloading malicious content.

**Analysis & Action**

Victims of a Vietnamese threat actor group named Ducktail are being lured into downloading information-stealing malware, such as DarkGate and RedLine. Ducktail lures in their victims by using fake LinkedIn posts and direct messaging about position offers from Corsair.

Ducktail mainly targets those in the US, UK, and India who have access to Facebook business accounts and hold positions in social media management. Through these direct messages and posts, victims are tricked into downloading malicious files that will attempt to uninstall security products and extract personal information from the compromised systems.

Members using LinkedIn are encouraged to verify the validity of approaching accounts and refresh staff memory on identifying suspicious LinkedIn accounts. Members can

also utilize the released list of indicators of compromise (IoCs) by WithSecure to decrease attacks from Ducktail.

Ragnar Locker Ransomware Developer Arrested in France

**Summary**

- The suspected developer of the Ragnar Locker ransomware group has been arrested in Paris, France.

**Analysis & Action**

On October 16, the key target of the Ragnar Locker ransomware group was arrested in Paris, while five other suspects are being interviewed in Spain and Latvia.

Ragnar's list of victims includes ADATA, Dassault Falcon, and Capcom. The ransomware group was responsible for targeting enterprises and operated semi-privately to attack at least 52 organizations in the critical infrastructure sector in the United States. As Ragnar Locker's infrastructure was seized, ransomware operations, such as the Trigona ransomware operation, were ceased, and stolen data was successfully retrieved by the Ukrainian Cyber Alliance (UCA).

While the Ragnar Locker ransomware group has been stopped, other ransomware groups are still at large. They mainly gain traction through phishing scams in emails by posing as legitimate senders from various organizations. To prevent other ransomware groups from stealing data and information, members are encouraged to refresh staff memory on identifying suspicious emails and downloads that could hide malicious intentions.

## Vulnerabilities & Exploits

Critical RCE Flaws Found in SolarWinds Access Audit Solution

**Summary**

- SolarWinds Access Rights Manager (ARM) has three critical Remote Code Execution (RCE) flaws.

**Analysis & Action**

Security researchers discovered three critical RCE vulnerabilities in the SolarWinds ARM system that could grant threat actors the ability to run code with SYSTEM privileges. SYSTEM level privileges are the highest-level privileges offered by the machine, similar root on Linux.

SolarWinds ARM is used to audit and manage user access across enterprise environments. The three vulnerabilities found were all classified as critical, with the most severe having a Common Vulnerability Scoring System (CVSS) score of 9.8/10.

SolarWinds has fixed the problem in their most recent ARM patch. Members are advised to make sure SolarWinds ARM products are running the most current version, Access Rights Manager 2023.2.1, to prevent exploitation of the three RCE vulnerabilities. To download the ARM patch, click here.

## Trends & Reports

September 2023 Healthcare Data Breach Report

**Summary**

- September saw the lowest number of reported healthcare data breaches since February 2023.

**Analysis & Action**

September saw the lowest number of reported healthcare data breaches since February 2023, with 48 breaches of 500 or more records reported to the HHS' Office for Civil Rights.

The largest data breaches within the healthcare industry can be attributed to the mass exploitation of a zero-day vulnerability in Progress Software's MOVEit solution, which is used by healthcare organizations and their vendors for transferring files. According to Emsisoft's research, out of 2,553 known organizations that were breached as a part of the MOVEit incident, 19.2% were in the healthcare sector.

It is expected that ransomware and extortion groups will continue to attack healthcare organizations. We encourage members to always back up their data, monitor their networks for suspicious activity, and work with their vendors and business collaborators in cybersecurity to be aware of any risks associated with supply chain compromise on their end.

## Privacy, Legal & Regulatory

- Nothing to Report

## Health-ISAC Cyber Threat Level

On September 20, 2023, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level at Blue (Guarded). The Threat Level of Blue (Guarded) is due to threats from concerns regarding malvertising, rogue USB drives, Async RAT, MFA Bypass, and persistent credential stuffing/spraying.

**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.**

---

**Reference | References**

**The Hacker News**
**Bleeping Computer**
**Bleeping Computer**
**Cisco**
**Bleeping Computer**
**Bleeping Computer**
**SolarWinds**
**HIPAA Journal**
**Health IT & CIO Report**

**Tags**

Corsair, okta, Lua, Cisco

---

**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 CSAP, please visit the Knowledge Base article CSAP Share Threat Intel Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

**Turn off Categories:**

For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

**Access the Health-ISAC 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 Cyware.

**For Questions or Comments:**

Please email us at toc@h-isac.org