Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: c3644cf6** **2022-10-11 13:02:45**

Today's Headlines:

Leading Story
- Critical Remote Code Execution Vulnerability Found in vm2 Sandbox Library

Data Breaches & Data Leaks
- State Bar of Georgia Confirms Data Breach Following Ransomware Attack

Cyber Crimes & Incidents
- US Airport Websites Hit by Suspected Pro-Russian Cyberattacks
- Caffeine Service Lets Anyone Launch Microsoft 365 Phishing Attacks

Vulnerabilities & Exploits
- Fortinet Warns of Active Exploitation of Newly Discovered Critical Auth Bypass Bug

Trends & Reports
- Callback Phishing Attacks Evolve Their Social Engineering Tactics
- US Government Announces New Cybersecurity Grant Program

Privacy, Legal & Regulatory
Nothing to Report

Upcoming Health-ISAC Events
- Health-ISAC Monthly Threat Brief – October 25, 2022, 12:00 PM Eastern

Leading Story

Critical Remote Code Execution Vulnerability Found in vm2 Sandbox Library

Summary

A critical vulnerability in vm2 may allow a remote attacker to escape the sandbox and execute arbitrary code on the host.

Analysis & Action

Security researchers with Oxeye discovered CVE-2022-36067, dubbed SandBreak, a critical-severity defect in vm2 assessed with a CVSS score of 10, which should put all vm2 users on alert due to its potential widespread impact.

The SandBreak vulnerability was addressed with the release of vm2 version 3.9.11 on August 28, but technical details on the bug have not been provided until now. Oxeye plans on publishing a technical blog post later this week.

AppSec engineers, R&D leaders, and security professionals should make sure that all vm2 sandbox instances within their environments are patched.

Additional insight is available here.

Data Breaches & Data Leaks

State Bar of Georgia Confirms Data Breach Following Ransomware Attack

Summary

> The State Bar of Georgia was hit by a ransomware attack earlier this year, and the organization has now confirmed that member and employee information was compromised.

Analysis & Action

Although described as a ransomware incident, no monetary demand appears to have been made by the attacker. However, the attacker shared current and former employee information that appears to have been stolen.

Exposed information includes names, addresses, dates of birth, social security numbers, driver's license numbers, direct deposit information, and name change information.

Impacted individuals are being offered free credit monitoring and identity protection services.

Cyber Crimes & Incidents

US Airport Websites Hit by Suspected Pro-Russian Cyberattacks

Summary

> The websites for several major US airports were briefly taken offline Monday after a cyberattack promoted by a pro-Russian hacking group.

Analysis & Action

Distributed Denial of Service (DDoS) attacks hit airport websites of several major US cities, including Atlanta, Chicago, New York, Phoenix, and St. Louis.

The airport websites were targeted after the pro-Russian hacktivist group KillNet published a list of sites and encouraged its followers to attack them.

Operations at the airports were not interrupted by the DDoS attacks.

Caffeine Service Lets Anyone Launch Microsoft 365 Phishing Attacks

Summary

> New phishing as a service (PhaaS) platform named Caffeine is making waves among security researchers for its effectiveness and ease of use.

Analysis & Action

Despite the evolving toolboxes of threat actors, the social engineering attack vector has remained the most popular attack method for the last few years. The PhaaS platform Caffeine creates an easily accessible avenue for novices to launch massive social engineering campaigns and for experienced groups to automate the first portion of a malicious campaign.

The rise in ‘as-a-service' entities expands far beyond social engineering. Ransomware as a service (RaaS), DDoS as a Service (DDoSaaS), and initial access vendors simplify the cyber threat landscapes for threat actors of every skill level.

As adversarial cyber action becomes more mainstream, the as-a-service market plays a significant role in weaponizing novices and aiding sophisticated threat actors. Caffeine marks the beginning of a new attack surface being weaponized. Members should be aware of the growing ease of launching cyber-attacks.

Vulnerabilities & Exploits

Fortinet Warns of Active Exploitation of Newly Discovered Critical Auth Bypass Bug

Summary

Fortinet revealed that the newly patched critical security vulnerability impacting its firewall and proxy products is being actively exploited in the wild.

Analysis & Action

The flaw, identified as CVE-2022-40684, relates to an authentication bypass in FortiOS, FortiProxy, and FortiSwitchManager. The flaw could allow a remote attacker to perform unauthorized operations on the administrative interface via specially crafted requests.

Impacted devices include:

- FortiOS version 7.2.0 through 7.2.1
- FortiOS version 7.0.0 through 7.0.6
- FortiProxy version 7.2.0
- FortiProxy version 7.0.0 through 7.0.6
- FortiSwitchManager version 7.2.0, and
- FortiSwitchManager version 7.0.0

If updating to the latest version is not an option, users should disable the HTTP/HTTPS administrative interface or limit IP addresses with access to the administrative interface.

Trends & Reports

Callback Phishing Attacks Evolve Their Social Engineering Tactics

Summary

Callback phishing operations have evolved their social engineering methods, keeping old fake subscriptions lure for the first phase of the attack but switching to pretending to help victims deal with an infection or hack.

Analysis & Action

BazarCall campaigns forgo malicious links or attachments in email messages in favor of phone numbers that recipients are misled into calling. The technique is reminiscent of vishing and tech support scams where potential victims were cold called by the attacker, except now, targeted users must dial the number.

Successful attacks infect victims with a malware loader that drops additional payloads such as remote access trojans, spyware, and ransomware.

Specific details on how social engineering call center campaigns operate are available for review here.

US Government Announces New Cybersecurity Grant Program

Summary

The White House has recently announced a $1 billion cybersecurity grant program designed to help state and local governments improve their cyber defenses, especially in protecting critical infrastructure.

Analysis and Action

The recent executive order stems from the $1.2 trillion infrastructure bill that was signed almost a year ago. That bill allocated $1 billion for protecting critical infrastructure against cyber-attack in the wake of a series of high-profile ransomware attacks such as the one that brought down the Colonial Pipeline.

Government agencies can take advantage of these funding opportunities but must use the funding to invest in new cybersecurity initiatives and local or rural communities.

While companies in the private sector are not eligible for these grants, the private sector will likely see an indirect benefit as an increased focus on cybersecurity will help IT security when addressing cyber threats.

Privacy, Legal & Regulatory

Nothing to Report

Health-ISAC Cyber Threat Level

On September 15, 2022, 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) was chosen in response to credential thieving and social engineering attempts with CEO Impersonation, fraudulent payment processing, EU energy crisis, Russia-Ukraine ongoing conflict, the railroad strike and supply chain Issues, and IcedID and Qbot

reemergence.

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(s): Security Week, Security Week, Security Week, Bleeping Computer, The Hacker News, Bleeping Computer, The Hacker News, Dark Reading, hornetsecurity

Tags: US Airports, Caffeine, State Bar of Georgia, vm2, callback campaigns, Daily Cyber Headlines, Government, DCH, Fortinet

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