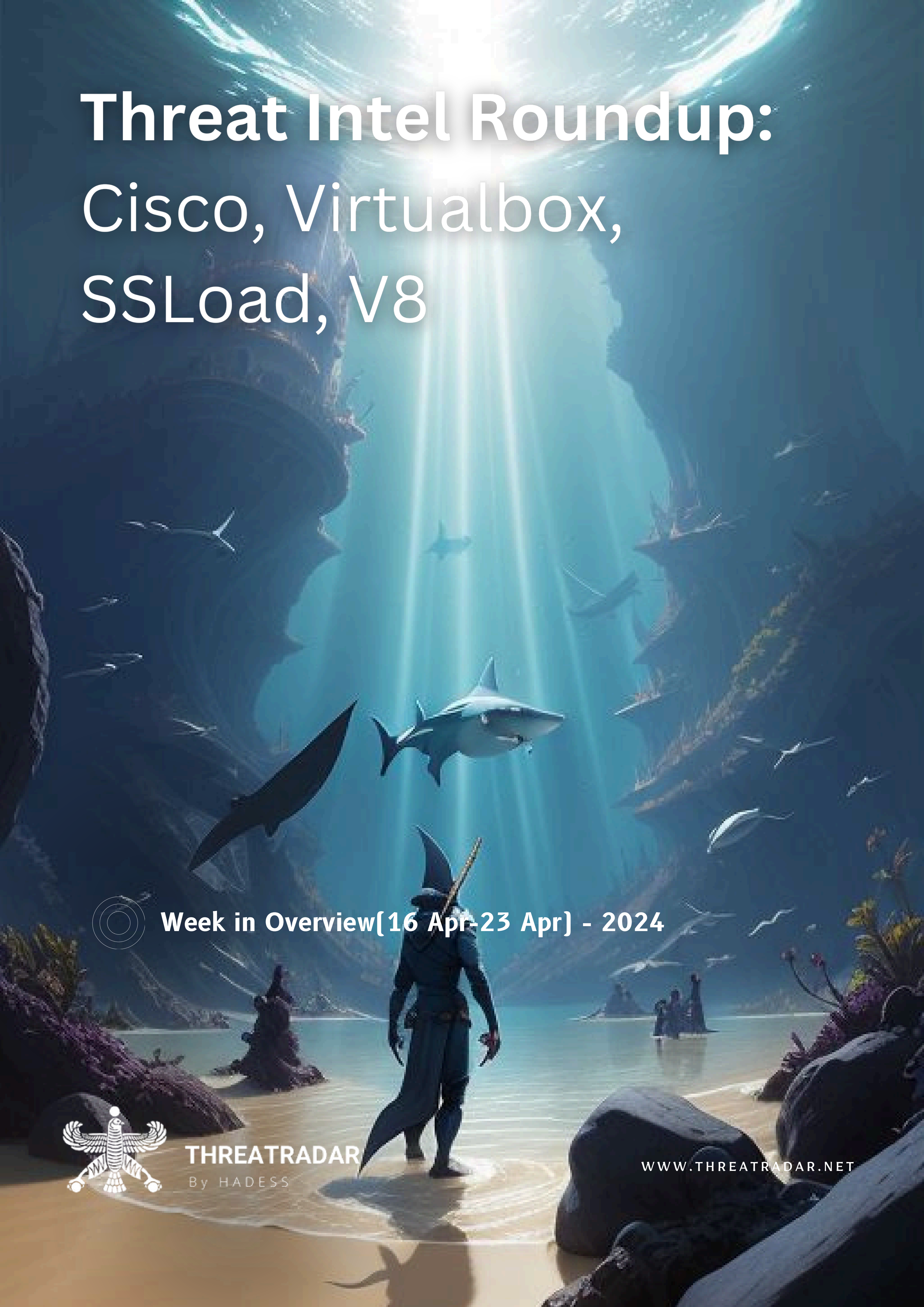


Threat Intel Roundup: Cisco, Virtualbox, SSLoad, V8

Week in Overview(16 Apr-23 Apr) - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. **Cisco C195 Email Security Appliance Vulnerabilities:**
    - The Cisco C195 is an Email Security Appliance (ESA) device designed to enhance network security by managing email traffic. However, recent exploration has revealed vulnerabilities in its security measures.
    - These vulnerabilities, yet to be specified, could potentially compromise the integrity and functionality of the Cisco C195 appliance, posing security risks to organizations relying on its email security capabilities.
    - Further research and analysis are required to fully understand the nature and extent of these vulnerabilities, along with potential mitigations to address them.
2. **SSLoad Malware:**
    - SSLoad is a type of malware that has been observed in cyberattacks targeting various systems.
    - Known for its sophistication, SSLoad malware is capable of evading detection and executing malicious actions on infected systems.
    - While specific details about SSLoad's capabilities and infection methods are not provided, it represents a significant cybersecurity threat that organizations should be aware of and take measures to defend against.
3. **CVE-2024-3400-RCE:**
    - CVE-2024-3400-RCE is a critical security vulnerability affecting Palo Alto Networks GlobalProtect, a widely used VPN solution.
    - This vulnerability allows remote attackers to execute arbitrary code on affected systems, potentially leading to complete compromise of the target network.
    - Organizations using Palo Alto Networks GlobalProtect are advised to apply security patches promptly to mitigate the risk of exploitation.
4. **CVE-2024-3832:**
    - CVE-2024-3832 is an object corruption vulnerability affecting WebAssembly (wasm) functions installation.
    - This vulnerability poses a risk to systems running wasm functions, potentially allowing attackers to manipulate objects and execute arbitrary code.
    - Specific details about the exploitation method and potential impact of CVE-2024-3832 are not provided, but organizations should monitor for security advisories and apply patches as they become available.
5. **CVE-2024-21111 in Oracle VirtualBox:**
    - CVE-2024-21111 is a critical vulnerability discovered in Oracle VirtualBox, a popular virtualization platform.
    - This flaw affects VirtualBox versions prior to 7.0.16 and allows attackers with basic access to a Windows system running VirtualBox to escalate their privileges.
    - A Proof-of-Concept (PoC) exploit has been made public, highlighting the urgency for users to update their VirtualBox installations to the latest version to mitigate the risk of exploitation.
    - Organizations relying on VirtualBox for virtualization should prioritize patching to protect against potential attacks leveraging CVE-2024-21111.

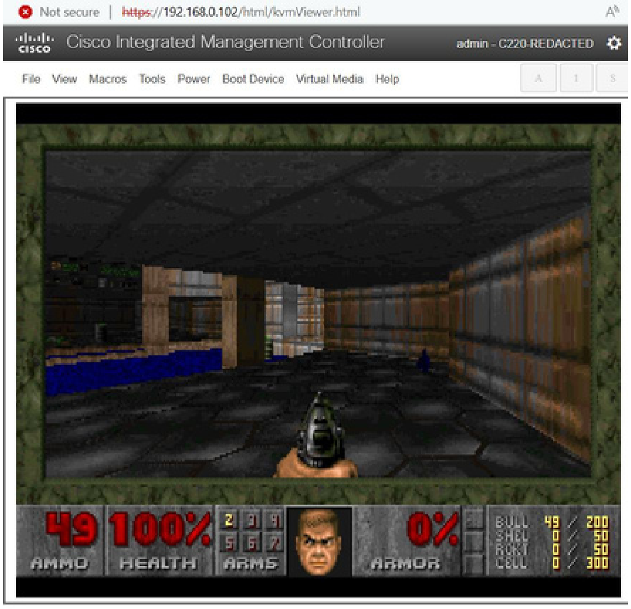
Key Findings

it is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- The Cisco C195 is a robust Email Security Appliance (ESA) Vulnerabilities
- SSLoad malware
- CVE-2024-3400-RCE is a critical security vulnerability that affects Palo Alto Networks GlobalProtect
- CVE-2024-3832, highlighting an object corruption vulnerability affecting WebAssembly (wasm) functions installation
- Proof-of-Concept (PoC) exploit for a critical vulnerability discovered in Oracle VirtualBox. Identified as CVE-2024-21111, this flaw affects VirtualBox versions prior to 7.0.16.

🚨 Vulnerability of the Week

Cisco CVE-2024-20356


Not secure | https://192.168.0.102/html/kvmViewer.html
Cisco Integrated Management Controller
admin - C220-REDACTED
File View Macros Tools Power Boot Device Virtual Media Help
49 AMMO
100% HEALTH
ARMS
0% ARMOR

The Cisco C195 is a robust Email Security Appliance (ESA) device designed to function as an SMTP gateway, enhancing network security by managing email traffic at the perimeter. Like other appliances in Cisco's range, the C195 is engineered with stringent security measures to prevent unauthorized code execution, ensuring the integrity of its operations. However, recent endeavors have seen individuals exploring the device's potential beyond its intended purpose.

In a notable adventure, a Cisco C195 appliance was disassembled with the aim of repurposing it as a general server. Despite assertions online that the device's secure boot mechanisms would thwart attempts to run alternate operating systems, innovative exploration led to a breakthrough. The Cisco C195 was successfully jailbroken, enabling the execution of unintended code. Central to this exploit was the discovery of a vulnerability within the CIMC (Cisco Integrated Management Controller) body management controller, identified as CVE-2024-20356. This vulnerability, when leveraged by an authenticated high-privilege user, grants root access to the server's BMC (Baseboard Management Controller), which holds considerable influence over various system components.

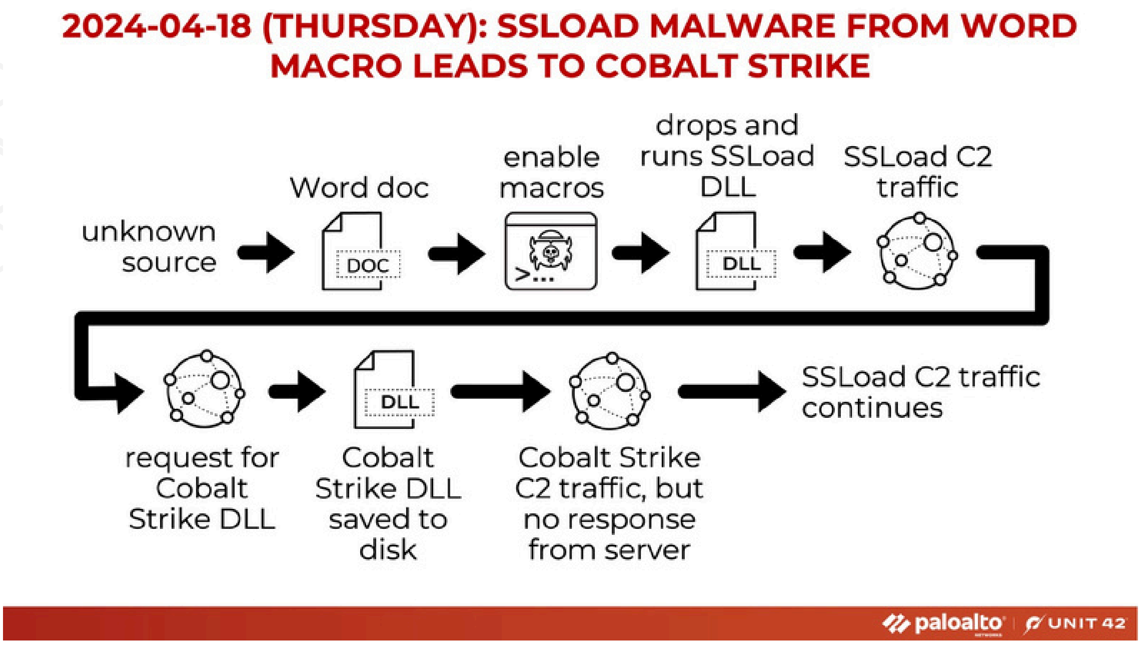
The ultimate objective of this endeavor was rather whimsical: to run the iconic video game DOOM on the Cisco C195 device. Following the successful jailbreak, a comprehensive toolkit for detecting and exploiting the CVE-2024-20356 vulnerability was released on GitHub, facilitating further exploration and experimentation.

One of the primary targets of this exploit chain was the BIOS (Basic Input/Output System), the firmware responsible for initializing hardware during the boot process. By examining different BIOS versions and assessing their impact on device operations, researchers sought to uncover potential attack surfaces and exploit vectors. Despite encountering challenges posed by the device's secure boot configuration, innovative techniques such as flash chip removal and DIY socket creation were employed to facilitate BIOS modification.

To mitigate the risk posed by such vulnerabilities, it is recommended to adhere to best practices such as changing default credentials, implementing strong password policies, and promptly updating devices to patch known vulnerabilities like CVE-2024-20356. By adopting proactive security measures, organizations can reduce the likelihood and impact of exploitation, safeguarding their network infrastructure from emerging threats.

https://twitter.com/Nettitude_Labs/status/1780990634687426932

Art of Detection


2024-04-18 (THURSDAY): SSLOAD MALWARE FROM WORD MACRO LEADS TO COBALT STRIKE
unknown source
Word doc
DOC
enable macros
>...
drops and runs SSLoad DLL
DLL
SSLoad C2 traffic
request for Cobalt Strike DLL
DLL
Cobalt Strike DLL saved to disk
Cobalt Strike C2 traffic, but no response from server
SSLoad C2 traffic continues
paloalto | UNIT 42

https://twitter.com/Unit42_Intel/status/1781326222019932535

On April 18, 2024, a sophisticated cyberattack campaign was observed, where an infection chain involving SSLoad malware ultimately led to attempted deployment of Cobalt Strike, a notorious tool used by threat actors for advanced persistent threats (APTs) and targeted attacks.

Infection Chain:

1. **Initial Compromise:** The infection began with an unknown vector, leading victims to interact with a Word document titled "Incident_Report_Harassment.doc," which contained malicious macros.
2. **Macro Execution:** Upon enabling macros, the Word document triggered the execution of SSLoad malware.
3. **SSLoad Execution:** The SSLoad DLL, identified by the code name "LosAngeles," was dropped and run on the infected system. A scheduled task was set up to ensure the SSLoad DLL restarted every ten minutes, maintaining persistence.
4. **Cobalt Strike Retrieval:** After establishing a connection with the command and control (C2) server, the infected host attempted to retrieve the Cobalt Strike DLL.
5. **Cobalt Strike Execution:** Despite successful retrieval, the Cobalt Strike DLL did not execute on the infected host. However, attempts to execute the DLL generated command and control (C2) traffic to a server that did not respond.

Associated Files:

1. **Incident_Report_Harassment.doc:** A Word document with macros to install the SSLoad malware.
2. **SSLoad DLL (64-bit):** Executable file dropped by the Word document and executed on the infected system. Located at "C:/Users/[username]/AppData/Local/Temp/app.pln."
3. **Cobalt Strike DLL (64-bit):** Retrieved from a remote server and intended for execution on the infected host. Located at "C:\Users[username]\AppData\Roaming\Microsoft\cNDbpXD\7bEGowXLibG.dll."

Infection Traffic:

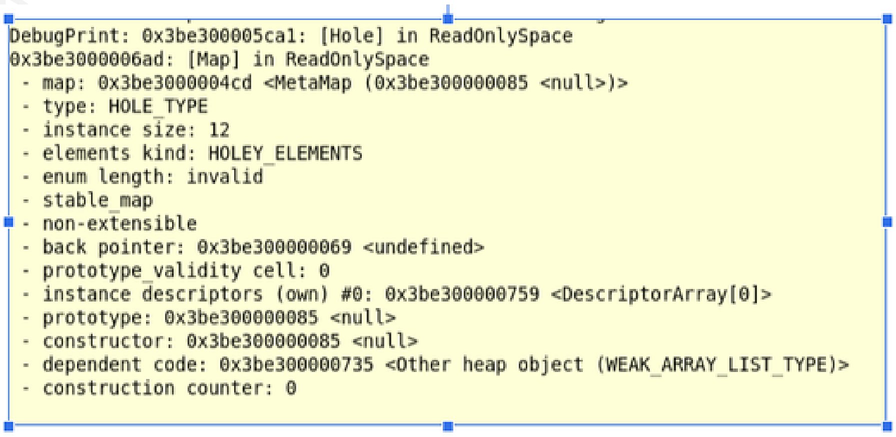
The infection traffic included communication over ports 443 and 80, with attempts to connect to various servers for command and control purposes. Notably, traffic to retrieve the Cobalt Strike DLL was observed on port 80, targeting the server at "212.18.104[.]28."

Cobalt Strike Traffic:

Upon attempted execution, the Cobalt Strike DLL generated traffic directed to the server at "193.32.176[.]22" over port 8080. However, no response was received from the server, indicating potential disruption or evasion tactics by the attackers.

This incident highlights the evolving sophistication of cyber threats, where multi-stage infection chains and attempts to deploy advanced tools like Cobalt Strike are used to infiltrate and compromise targeted systems. Organizations are urged to remain vigilant and implement robust cybersecurity measures to defend against such threats.

1Day



```
DebugPrint: 0x3be300005ca1: [Hole] in ReadOnlySpace
0x3be3000006ad: [Map] in ReadOnlySpace
 - map: 0x3be3000004cd <MetaMap (0x3be300000085 <null>)>
 - type: HOLE_TYPE
 - instance size: 12
 - elements kind: HOLEY_ELEMENTS
 - enum length: invalid
 - stable_map
 - non-extensible
 - back pointer: 0x3be300000069 <undefined>
 - prototype_validity cell: 0
 - instance descriptors (own) #0: 0x3be300000759 <DescriptorArray[0]>
 - prototype: 0x3be300000085 <null>
 - constructor: 0x3be300000085 <null>
 - dependent code: 0x3be300000735 <Other heap object (WEAK_ARRAY_LIST_TYPE)>
 - construction counter: 0
```

https://twitter.com/buptdsb/status/1782565495851589757

A security advisory has been issued regarding CVE-2024-3832, highlighting an object corruption vulnerability affecting WebAssembly (wasm) functions installation. This vulnerability, reported by Man Yue Mo of GitHub Security Lab, was disclosed on March 27, 2024. The issue arises due to object corruption in V8, the JavaScript engine used in Google Chrome and other Chromium-based browsers.

The vulnerability allows for the manipulation of wasm functions during installation, leading to potential object corruption. While no Proof-of-Concept (PoC) has been provided, the vulnerability's severity is underscored by its classification as "High" and the reward of $20,000 offered for its discovery.

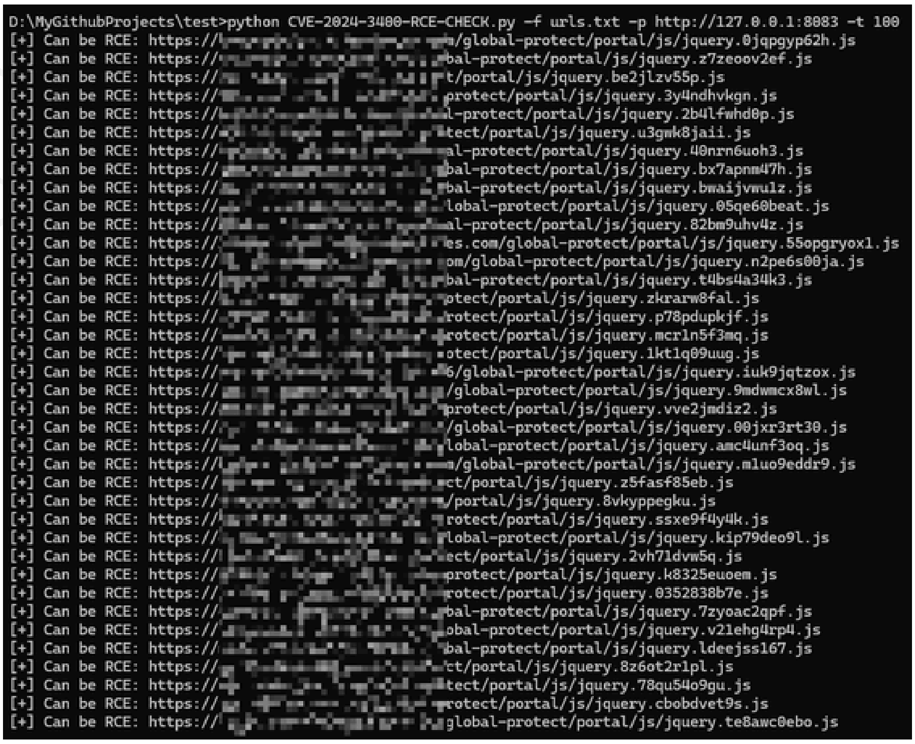
The vulnerability involves a scenario where installing wasm functions can cause object corruption, potentially leading to security breaches. The exploit revolves around the manipulation of properties and elements within JavaScript objects, specifically targeting the WebAssembly global object.

Previous similar vulnerabilities, such as CVE-2021-30561 and CVE-2022-1486, have been reported, indicating a recurring pattern of object corruption issues in the context of JavaScript and wasm integration. Efforts to address this vulnerability include adding runtime name collision checks and implementing safeguards during property appending to prevent the creation of corrupted JavaScript objects. Additionally, historical write-ups, such as CVE-2023-2935, provide insights into similar exploitation techniques involving duplicate property primitives and object reshuffling.

The vulnerability analysis suggests potential exploitation avenues through type confusion and object reshuffling, emphasizing the need for thorough mitigation measures to protect against malicious attacks leveraging this vulnerability.

Ultimately, the security community's ongoing efforts to identify and address vulnerabilities in JavaScript engines like V8 highlight the importance of continuous security research and proactive vulnerability management to safeguard against emerging threats.

NDay



```
D:\MyGithubProjects\test>python CVE-2024-3400-RCE-CHECK.py -f urls.txt -p http://127.0.0.1:8083 -t 100
[+] Can be RCE: https://[redacted]n/global-protect/portal/js/jquery.0jqpgyp62h.js
[+] Can be RCE: https://[redacted]bal-protect/portal/js/jquery.z7zeoov2ef.js
[+] Can be RCE: https://[redacted]t/portal/js/jquery.be2jlzv55p.js
[+] Can be RCE: https://[redacted]protect/portal/js/jquery.3y4ndhvkgn.js
[+] Can be RCE: https://[redacted]l-protect/portal/js/jquery.2b4lfwhd0p.js
[+] Can be RCE: https://[redacted]tect/portal/js/jquery.u3gmk8jaii.js
[+] Can be RCE: https://[redacted]al-protect/portal/js/jquery.40nrn6uoh3.js
[+] Can be RCE: https://[redacted]bal-protect/portal/js/jquery.bx7apnm47h.js
[+] Can be RCE: https://[redacted]bal-protect/portal/js/jquery.bwaijvwulz.js
[+] Can be RCE: https://[redacted]lobal-protect/portal/js/jquery.05qe60beat.js
[+] Can be RCE: https://[redacted]al-protect/portal/js/jquery.82bm9uhv4z.js
[+] Can be RCE: https://[redacted]es.com/global-protect/portal/js/jquery.55opgryox1.js
[+] Can be RCE: https://[redacted]om/global-protect/portal/js/jquery.n2pe6s00ja.js
[+] Can be RCE: https://[redacted]bal-protect/portal/js/jquery.t4bs4a34k3.js
[+] Can be RCE: https://[redacted]otect/portal/js/jquery.zkrarw8fal.js
[+] Can be RCE: https://[redacted]rotect/portal/js/jquery.p78pdupkjf.js
[+] Can be RCE: https://[redacted]rotect/portal/js/jquery.mcr1n5f3mq.js
[+] Can be RCE: https://[redacted]otect/portal/js/jquery.1kt1q09uug.js
[+] Can be RCE: https://[redacted]6/global-protect/portal/js/jquery.iuk9jqtzox.js
[+] Can be RCE: https://[redacted]/global-protect/portal/js/jquery.9mdwmcx8wl.js
[+] Can be RCE: https://[redacted]protect/portal/js/jquery.vve2jmdiz2.js
[+] Can be RCE: https://[redacted]/global-protect/portal/js/jquery.00jxr3rt30.js
[+] Can be RCE: https://[redacted]lobal-protect/portal/js/jquery.amc4unf3oq.js
[+] Can be RCE: https://[redacted]n/global-protect/portal/js/jquery.m1uo9eddr9.js
[+] Can be RCE: https://[redacted]ct/portal/js/jquery.z5fasf85eb.js
[+] Can be RCE: https://[redacted]/portal/js/jquery.8vkyppegku.js
[+] Can be RCE: https://[redacted]rotect/portal/js/jquery.ssxe9f4y4k.js
[+] Can be RCE: https://[redacted]lobal-protect/portal/js/jquery.kip79deo9l.js
[+] Can be RCE: https://[redacted]ect/portal/js/jquery.2vh71dvw5q.js
[+] Can be RCE: https://[redacted]protect/portal/js/jquery.k8325euoem.js
[+] Can be RCE: https://[redacted]rotect/portal/js/jquery.0352838b7e.js
[+] Can be RCE: https://[redacted]bal-protect/portal/js/jquery.7zyoac2qpf.js
[+] Can be RCE: https://[redacted]obal-protect/portal/js/jquery.v21ehg4rp4.js
[+] Can be RCE: https://[redacted]bal-protect/portal/js/jquery.1deejss167.js
[+] Can be RCE: https://[redacted]ct/portal/js/jquery.8z6ot2r1pl.js
[+] Can be RCE: https://[redacted]tect/portal/js/jquery.78qu54o9gu.js
[+] Can be RCE: https://[redacted]rotect/portal/js/jquery.cbobdvet9s.js
[+] Can be RCE: https://[redacted]global-protect/portal/js/jquery.te8awc0ebo.js
```

https://twitter.com/W01fh4cker/status/1782346896088125442

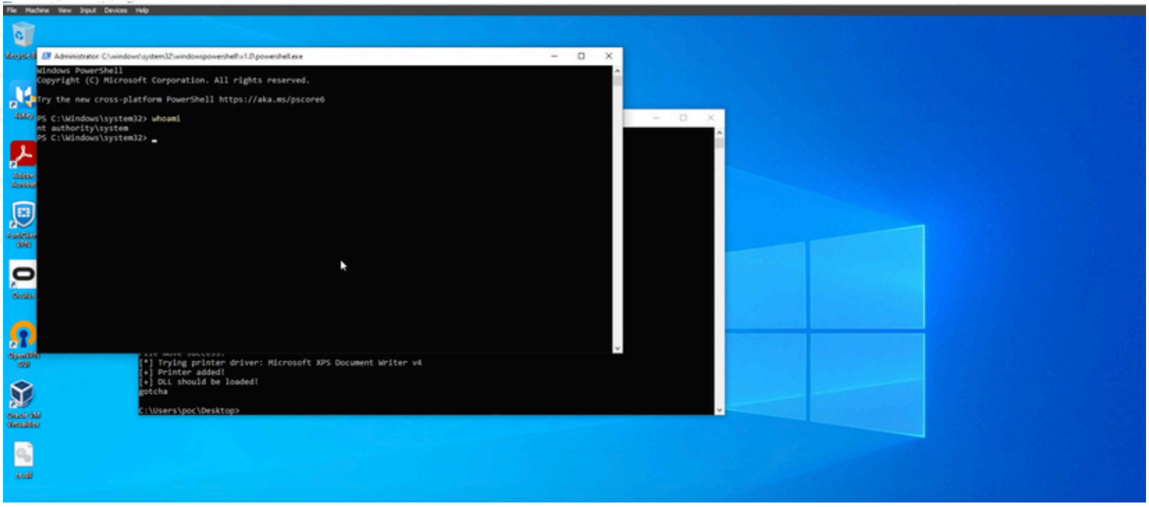
CVE-2024-3400-RCE is a critical security vulnerability that affects Palo Alto Networks GlobalProtect, a widely used VPN solution. This vulnerability allows remote attackers to execute arbitrary code on affected systems, potentially leading to complete compromise of the target network.

The vulnerability was discovered through a technique known as "Cyberspace Mapping Dork," which involves using specialized search engines like Fofa, Zoomeye, Hunter.how, and Shodan to identify systems running vulnerable software.

- **Fofa**: A search for "app='paloalto-GlobalProtect'" reveals potentially vulnerable instances of Palo Alto GlobalProtect portals.
- **Zoomeye**: A search for "app:'Palo Alto Networks firewall httpd'" provides further insight into systems that may be exposed to the vulnerability.
- **Hunter.how**: By searching for "product.name='GlobalProtect Portal'", additional vulnerable instances can be identified.
- **Shodan**: A search for "http.favicon.hash:-631559155" helps to uncover systems potentially running GlobalProtect.

To check for the vulnerability, a Python script named CVE-2024-3400-RCE-CHECK.py is provided. This script scans a list of URLs specified in a text file and attempts to exploit the vulnerability by connecting to the target systems using the provided payload and port.
References to further information and analysis of the vulnerability are provided via GitHub repositories, AttackerKB, and Watchtower Labs. These resources offer details on the vulnerability's exploitation, potential impact, and mitigation strategies.

🌶️ Trending Exploit



File Machine View Input Devices Help
Administrator: C:\windows\system32\windowspowershell\v1.0\powershell.exe

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> whoami
nt authority\system
PS C:\Windows\system32> _
```

```
[*] Trying printer driver: Microsoft XPS Document Writer v4
[+] Printer added!
[+] DLL should be loaded!
gotcha

C:\Users\poc\Desktop>
```

https://twitter.com/the_yellow_fall/status/1782326866977886467

A security researcher has recently disclosed a Proof-of-Concept (PoC) exploit for a critical vulnerability discovered in Oracle VirtualBox. Identified as CVE-2024-21111, this flaw affects VirtualBox versions prior to 7.0.16. It poses a significant threat as it enables attackers with limited access to a Windows system hosting VirtualBox to escalate their privileges.

The exploit code has been made publicly available on GitHub by the researcher, raising concerns about potential exploitation by malicious actors. This revelation underscores the importance of promptly updating VirtualBox installations to the latest secure version to mitigate the risk posed by this vulnerability.

🕯️ The Topic of the Week

https://twitter.com/404mediaco/status/1782461511140524319

In the lead-up to the release of Taylor Swift's album "The Tortured Poets Department," the singer-songwriter sparked a buzz within both her fanbase and an unexpected community: vintage typewriter enthusiasts. Swift's teaser video, featuring her typing the words "as she was leaving it felt like breathing" on a typewriter, ignited speculation among fans and typewriter aficionados alike.

Members of typewriter-focused online forums and social media groups expressed mixed reactions to Swift's typewriter-themed promotional content. Some expressed concern over a potential surge in demand for typewriters, anticipating higher prices and competition for vintage models. Others welcomed the attention, viewing it as an opportunity to introduce newcomers to the hobby and preserve interest in vintage typewriters for future generations.

The release of Swift's music video for "Fortnight," featuring typewriter scenes with Post Malone, further fueled discussions within the typewriter community. Identified as a Royal 10, the typewriter featured in Swift's promotional materials led enthusiasts to speculate about its history and value.

Swift's frequent references to typewriters in her music and promotional materials, including lyrics mentioning the "Tortured Poets Department" and imagery of her using typewriters, added to the intrigue. While some worried about a potential influx of inexperienced buyers, others noted the hobby's resilience over the years, citing periodic surges in popularity and the enduring appeal of vintage typewriters.

Despite concerns, many in the typewriter community remained optimistic about the hobby's future. Some saw Swift's influence as an opportunity to educate newcomers and foster a deeper appreciation for typewriters' craftsmanship and history. Ultimately, the community hoped that Swift's involvement would spark renewed interest in typewriters and contribute to their preservation for years to come.

HADESS

cat /etc/HADESS

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:	Threat Radar
WWW.HADESS.IO	**WWW.THREATRADAR.NET**

Threat Radar is a powerful threat intelligence platform that combines advanced analytics, machine learning, and human expertise to deliver actionable intelligence to organizations. It continuously monitors various data sources, including the deep web, dark web, social media platforms, and open-source intelligence, to identify potential threats, vulnerabilities, and emerging attack patterns.