WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

CRITICAL SECURITY VULNERABILITY IN 'ULTIMATE MEMBER' PLUGIN PUTS OVER 200,000 WORDPRESS SITES AT RISK

A critical security flaw, CVE-2023-3460, has been identified in the widely used 'Ultimate Member' plugin, posing a significant threat to website owners. Attackers are exploiting this vulnerability, allowing them to create unauthorized user accounts with administrator privileges. As a result, over 200,000 WordPress websites are currently at risk.

This article aims to raise awareness among site owners about the severity of the issue and provide mitigation measures.

The 'Ultimate Member' plugin streamlines WordPress registration and login, but has a flaw (CVE-2023-3460) enabling hackers to create privileged accounts. Suspicious account creation since June suggests active exploitation.

Exploiting the Vulnerability:
The 'Ultimate Member' plugin contains a critical security flaw, tracked as CVE-2023-3460. This flaw allows attackers to create unauthorized user accounts with administrator-level privileges. Users of the plugin have reported the creation of suspicious accounts since June, indicating active exploitation of this vulnerability.

Description: Ultimate Member <= 2.6.6 – Privilege Escalation via Arbitrary User Meta Updates

Affected Plugin: Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin

Plugin Slug: ultimate-member

Affected Versions: <= 2.6.6

CVE ID: CVE-2023-3460

CVSS Score: 9.8 (Critical)

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

Simply put, the 'Ultimate Member' plugin vulnerability allows hackers to gain unauthorized control by creating admin-level accounts. Website owners must act quickly to protect their sites from further unauthorized access.

Root Cause of the Issue:
The vulnerability in the 'Ultimate Member' plugin stems from a conflict between its blocklist logic and how WordPress handles metadata keys. WordPress is a widely used content management system (CMS) for websites. Metadata keys are tags attached to data that provide additional context. The plugin uses blocklists to protect specific metadata keys from being changed during account creation. Attackers exploit the discrepancy between the plugin and WordPress by manipulating metadata keys, gaining unauthorized access and carrying out malicious activities.

Patching Efforts and Acknowledgment:
The 'Ultimate Member' plugin maintainers have made attempts to address the vulnerability in the last two versions but haven't fully patched the flaw. However, they have acknowledged the ongoing exploitation of the vulnerability in real-world scenarios.

Mitigation Measures for Site Owners:
Site owners are strongly advised to disable the 'Ultimate Member' plugin to protect their websites from potential exploitation. Conducting a thorough audit of administrator roles is also recommended to identify any rogue accounts that may have been created.

In Conclusion, the critical security vulnerability CVE-2023-3460 in the 'Ultimate Member' plugin poses a significant risk to over 200,000 WordPress websites. Site owners must understand the seriousness of the issue, disable the vulnerable plugin, and conduct thorough website audits to mitigate potential security risks.

Prioritizing security measures and implementing robust solutions is crucial for protecting WordPress websites and user data. Armoryze offers comprehensive **web application and API protection services**, along with **risk-based vulnerability management services**. Partnering with Armoryze can fortify your website's defenses and proactively prevent vulnerability exploitation.

Take proactive steps to ensure the safety and integrity of your website. Schedule a **FREE consultation** with Armoryze today to discuss your security needs and develop a tailored strategy for protecting your WordPress website and its valuable data.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

BLACKCAT RANSOMWARE EXPLOITS WINSCP SEARCH ADS TO DISTRIBUTE COBALT STRIKE: A COMPREHENSIVE ANALYSIS

In a recent development, the BlackCat ransomware group, also known as ALPHV, has employed malvertizing campaigns to deceive unsuspecting users. By capitalizing on the popularity of the widely-used file-transfer application WinSCP, they have distributed malware-infected files through counterfeit websites resembling the official WinSCP site.

This article explores the tactics employed by the BlackCat ransomware group, highlights the risks faced by system administrators and IT professionals, and uncovers the subsequent stages of the attack.

Exploiting the Popularity of WinSCP:
WinSCP (Windows Secure Copy), a popular file-transfer application for Windows, is renowned for its user-friendly interface, encryption capabilities, and support for automation. It offers secure file transfer using protocols like SFTP (SSH File Transfer Protocol), FTP (File Transfer Protocol), SCP (Secure Copy Protocol), and Amazon S3. Moreover, it serves as a file manager for remote servers and cloud storage. Regrettably, the BlackCat ransomware group exploits WinSCP's reputation to target valuable corporate networks.

The Deceptive Strategy:
BlackCat ransomware operators run ad campaigns on Google and Bing, manipulating search results for "WinSCP Download." Users unknowingly click on malicious ads, leading them to deceptive tutorial websites designed to evade Google's detection.

Cloned Websites and Malware Distribution:
Counterfeit tutorial sites mimic the official WinSCP website using similar domain names. They lure users into downloading malware by displaying a deceptive download button. Clicking it downloads an ISO file containing "setup.exe" and "msi.dll." The distraction of "setup.exe" masks the activation of the malware dropper, "msi.dll."

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

Execution and Malicious Payload:
When "setup.exe" is run, it extracts a disguised Python folder from "msi.dll." This folder appears as a genuine WinSCP installer. The installation process includes a trojanized python310.dll file and establishes persistence by creating a run key named "Python" with the value "C:\Users\Public\Music\python\pythonw.exe." The executable pythonw.exe loads an obfuscated python310.dll containing a Cobalt Strike beacon to connect with a command-and-control server.

Advanced Tools and Lateral Movement:
The BlackCat ransomware group proceeds with their malicious activities after gaining access with the Cobalt Strike beacon. Trend Micro analysts have identified their use of diverse tools and techniques in subsequent attack phases.

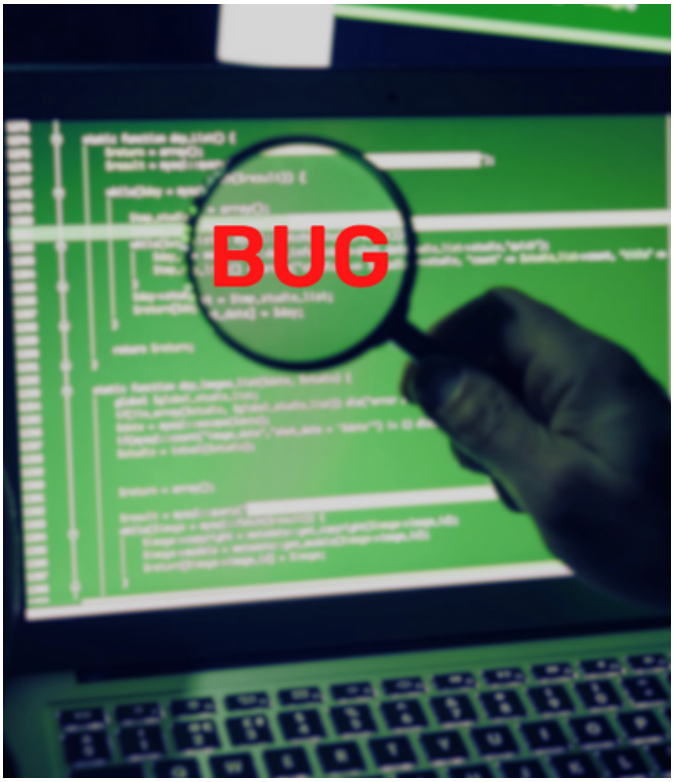
- AdFind: A command-line tool utilized to retrieve information from Active Directory (AD).
- PowerShell commands: Employed for data gathering, ZIP file extraction , and script execution.
- Python scripts: Used to assess and examine user and group permissions through AccessChk64.
- Findstr: Utilized for searching passwords within XML files.
- PowerView: A PowerSploit script used for Active Directory reconnaissance and enumeration.
- Python scripts: Employed to retrieve passwords and acquire Veeam credentials using the LaZagne tool.
- PsExec, BitsAdmin, and Curl: Tools used for navigating and moving within compromised networks.
- AnyDesk: A legitimate remote management tool manipulated by attackers to ensure their continued access and control over compromised systems.
- KillAV BAT script: Designed to disable or bypass antivirus and antimalware programs.
- PuTTY Secure Copy client: Used for exfiltrating collected information from compromised systems.

The BlackCat ransomware group uses advanced tools and techniques for network movement, data gathering, privilege escalation, and persistence. To protect against such threats, it is crucial to stay vigilant, update software, educate users, and implement security measures. Armoryze offers a **Managed Detection and Ransomware Service** with expert monitoring and incident response. Act now to fortify your defenses. Contact us for a **FREE consultation.**

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

MITRE UNVEILS THE TOP 25 MOST DANGEROUS SOFTWARE BUGS



MITRE has released its highly anticipated list of the top 25 most perilous software bugs, revealing critical weaknesses that have plagued software systems in recent years. These vulnerabilities pose severe threats to the security and stability of affected devices, making it essential for individuals, organizations, and developers to address them promptly.

MITRE's evaluation of thousands of CVE entries highlights the most dangerous weaknesses, enabling us to understand their potential impact and take proactive measures to safeguard our systems.These findings serve as a valuable resource for prioritizing security efforts and allocating resources to address the most critical vulnerabilities.

Software weaknesses encompass various flaws, bugs, vulnerabilities, and errors that can compromise the integrity and security of the systems they reside in. These weaknesses provide malicious actors with potential entry points to gain control over affected devices, extract sensitive data, or cause denial-of-service states. To raise awareness about these critical issues, MITRE has evaluated 43,996 CVE entries from the National Vulnerability Database (NVD) and CISA's Known Exploited Vulnerabilities (KEV) catalog, focusing on vulnerabilities discovered and reported between 2021 and 2022.

After meticulous analysis, MITRE has assigned scores to each weakness based on their severity and prevalence. By normalizing the frequency and severity values relative to the dataset, MITRE has developed a ranking formula to determine the top 25 most dangerous software bugs. The severity is measured using the Common Vulnerability Scoring System (CVSS) score, ensuring a comprehensive evaluation of each vulnerability's impact.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

The Top 25 Dangerous Bugs:

Rank	CWE ID	Name	Score	CVEs in KEV	Rank Change
1	CWE-787	Out-of-bounds Write	63.72	70	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.54	4	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	34.27	6	0
4	CWE-416	Use After Free	16.71	44	+3
5	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15.65	23	+1
6	CWE-20	Improper Input Validation	15.50	35	-2
7	CWE-125	Out-of-bounds Read	14.60	2	-2
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.11	16	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.73	0	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	10.41	5	0
11	CWE-862	Missing Authorization	6.90	0	+5
12	CWE-476	NULL Pointer Dereference	6.59	0	-1
13	CWE-287	Improper Authentication	6.39	10	+1
14	CWE-190	Integer Overflow or Wraparound	5.89	4	-1
15	CWE-502	Deserialization of Untrusted Data	5.56	14	-3
16	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	4.95	4	+1
17	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.75	7	+2
18	CWE-798	Use of Hard-coded Credentials	4.57	2	-3
19	CWE-918	Server-Side Request Forgery (SSRF)	4.56	16	+2
20	CWE-306	Missing Authentication for Critical Function	3.78	8	-2
21	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.53	8	+1
22	CWE-269	Improper Privilege Management	3.31	5	+7
23	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.30	6	+2
24	CWE-863	Incorrect Authorization	3.16	0	+4
25	CWE-276	Incorrect Default Permissions	3.16	0	-5

These critical vulnerabilities have had a significant impact on software released in the past two years, enabling attackers to gain control, exfiltrate data, or launch debilitating DoS attacks. MITRE shares this list to raise awareness and emphasize the urgent need to address these software security weaknesses.

Armoryze, a trusted leader in cybersecurity, recognizes the importance of safeguarding systems against these dangerous software bugs. With our comprehensive Managed Security Services, we offer tailored solutions to proactively identify, mitigate, and protect against vulnerabilities and potential cyber threats. Our experienced professionals collaborate closely with clients to develop robust security strategies, implement proactive monitoring, and ensure ongoing protection of valuable assets.

To fortify your defenses against the top software vulnerabilities highlighted by MITRE, leverage the expertise of Armoryze **Managed Security Services**. Don't leave your systems vulnerable to malicious attacks—take action today. **Contact us** now to schedule a consultation and secure your digital infrastructure.

Remember, staying one step ahead in the battle against cyber threats requires constant vigilance. Stay informed, stay protected, and partner with Armoryze security services to strengthen your defenses.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

UNVEILING SMUGX: CHINESE HACKERS TARGET EUROPEAN GOVERNMENT ENTITIES

In the face of a relentless wave of cyber threats targeting European government entities, Armoryze brings to light the alarming SmugX phishing campaign orchestrated by Chinese hackers. This blog article reveals the insidious tactics employed by the campaign, exposes the threat actor behind it, and emphasizes the urgent need for robust cybersecurity measures.

The Targeted Entities:
The SmugX campaign has specifically targeted embassies and foreign affairs ministries across Europe since December 2022, focusing on countries such as the United Kingdom, France, Sweden, Ukraine, Czech Republic, Hungary, and Slovakia. These calculated attacks demand immediate attention and proactive defense.

Decoding the SmugX Attack Chains:
Security researchers have conducted a meticulous analysis of the SmugX attacks, uncovering two primary infection chains utilized by the campaign. Understanding these attack chains is crucial in comprehending the gravity of the threat they pose to organizations.

SMUGX Variant 1 :
ZIP Archive and DLL Sideloading: SmugX uses a deceptive method involving a ZIP archive to deploy its malicious payload. When victims open the ZIP file, PowerShell is executed, extracting the archive's contents to a temporary folder. The archive contains innocent-looking files, such as "robotaskbaricon.exe" or "passwordgenerator.exe," which hide a malicious DLL named "Roboform.dll." Through DLL sideloading, the legitimate program loads the Roboform.dll file, activating the dangerous PlugX remote access trojan (RAT). This RAT grants attackers remote control, unauthorized access, and potential data theft.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

SMUGX Variant 2:
HTML Smuggling and MSI Download: In this SmugX variant, threat actors use HTML smuggling to secretly download a JavaScript file. The JavaScript file triggers the download of an MSI file, creating a new folder on the victim's computer. Within this folder, three files are placed: a modified legitimate program, a loader DLL, and an encrypted malicious payload called 'data.dat.' DLL sideloading is utilized to load the malicious payload into memory, while a hidden directory and 'Run' registry key entry conceal their activities. The PlugX malware may also display a misleading PDF file for diversion and reduced detection.

The Notorious PlugX Remote Access Trojan (RAT):
At the core of the SmugX campaign lies the notorious PlugX RAT, a modular remote access trojan associated with Chinese advanced persistent threat (APT) groups since 2008. This adaptable malware enables threat actors to carry out file exfiltration, screenshot capture, keylogging, and remote command execution. The version employed in the SmugX campaign exhibits similarities to recent Chinese adversary attacks, indicating a growing interest in European targets and espionage as the likely motive.

In conclusion, the SmugX campaign poses a grave threat to European government entities, highlighting the critical need to strengthen cybersecurity measures. Armoryze, a leading cybersecurity company, is dedicated to safeguarding clients and mitigating risks. With cutting-edge **SIEM logging and monitoring services**, our cybersecurity specialists proactively detect and respond to potential security breaches. We assess your organization's security posture and develop tailored security solutions to protect your critical assets. Partner with Armoryze today through a **FREE consultation** with our cybersecurity specialists to fortify your defenses against sophisticated cyber threats. Take the first step towards a more secure future.

Stay vigilant, keep your systems updated, and together let's protect your organization from the evolving cyber threat landscape.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

PROTECTING PHOTOVOLTAIC MONITORING SYSTEMS FROM CYBER ATTACKS: BEST PRACTICES AND SECURITY MEASURES

Photovoltaic (PV) monitoring systems are crucial for managing renewable energy production units. However, the exposure of these systems on the public web has made them vulnerable to cyber attacks. In this blog article, we will address the risks associated with exposed PV systems and provide best practices and security measures to enhance their protection against potential hackers.

Scope of the Issue:
Cyble's findings reveal 134,634 internet-exposed PV products from vendors like Solar-Log, Danfoss Solar Web Server, and SMA Sunny Webbox. Unauthenticated visitors can access sensitive information and settings, increasing the risk of attacks. Older firmware versions contain vulnerabilities, amplifying the likelihood of exploitation.

Recent Exploitations and Botnet Activity:
Recent incidents have demonstrated the real-world risks associated with exposed PV systems. For instance, hackers have targeted vulnerable devices to add them to botnets. CVE-2022-29303, an unauthenticated remote command injection vulnerability in Contec's SolarView system, was exploited by a new variant of the Mirai botnet. It's essential to note that this vulnerability is not an isolated case, as other unauthenticated remote code execution vulnerabilities have also been discovered, such as CVE-2023-23333.

Mitigating Risks and Enhancing Security: To minimize the potential for cyber attacks on PV monitoring systems, administrators should implement the following best practices:

1. Strong and Unique Credentials: Access to system interfaces should be protected with strong, unique passwords. Default or easily guessable credentials should be avoided to prevent unauthorized access.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

2.Multi-Factor Authentication: Activate multi-factor authentication where available. This additional layer of security requires users to provide an extra verification, such as a unique code sent to their mobile devices, along with their credentials.

3.Regular System Updates: Keep PV systems up to date with the latest firmware versions and security patches. Regularly check for updates from system vendors and apply them promptly to address known vulnerabilities.

4.Network Segregation: Isolate PV monitoring equipment from other critical infrastructure by segregating it onto its own network. This practice limits the potential impact of a successful breach by restricting attackers' lateral movement.

In Conclusion, the exposure of tens of thousands of PV monitoring systems on the public web poses a significant risk to the renewable energy sector. Implementing security measures such as strong credentials, multi-factor authentication, regular updates, and network segregation can greatly enhance the protection of these systems against cyber attacks. Armoryze, a leading cybersecurity company, understands the importance of securing infrastructure and offers comprehensive **risk-based vulnerability management services** to help organizations proactively manage their security posture and stay ahead of potential risks.

Contact us today to learn more about how our services can protect your PV monitoring systems, ensure uninterrupted operation, and safeguard your renewable energy production units. Don't leave your systems vulnerable to attacks. Act now to protect your infrastructure and contribute to the overall security of the renewable energy industry.

Don't Wait Until It's Late. Contact Us Today.

info@armoryze.co.uk +44-0208 427 1131