Threat Intel Roundup: PwnOverWifi, GravityRAT, BadSpace, iconv

Week in Overview[11 Jun-18 Jun] - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

CVE-2024-6044 and CVE-2024-6045 Vulnerabilities in D-Link EAGLE PRO AI and AQUILA PRO AI Devices
Two critical vulnerabilities, CVE-2024-6044 and CVE-2024-6045, have been identified in the D-Link EAGLE PRO AI and AQUILA PRO AI device families. These vulnerabilities allow for LAN-side arbitrary file reading and elevated unauthenticated access.

BadSpace Malware Delivered via Compromised Websites
BadSpace is a Windows backdoor malware distributed through compromised websites masquerading as fake browser updates.

GravityRAT and HeavyLift Malware Threat Analysis
GravityRAT, a remote access trojan, has evolved to include Android targeting capabilities and integrates with HeavyLift, an Electron-based malware loader.

Critical Vulnerability in PHP - CVE-2024-2961
CVE-2024-2961 is a critical vulnerability in PHP's iconv() function, which can be exploited through various means including the symfony/polyfill-mbstring library.

Forest Compromise Through AMA Abuse
Forest compromise through AMA (Azure Monitor Agent) abuse involves exploiting misconfigurations and vulnerabilities in Azure environments.

Critical Security Updates for Microsoft
Microsoft has released critical security updates to address multiple vulnerabilities across various products.

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:

- Advisory: CVE-2024-6044 and CVE-2024-6045 Vulnerabilities in D-Link EAGLE PRO AI and AQUILA PRO AI Devices
- Advisory: BadSpace Malware Delivered via Compromised Websites
- Advisory: GravityRAT and HeavyLift Malware Threat Analysis
- Advisory: Critical Vulnerability in PHP - CVE-2024-2961
- Advisory: Forest Compromise Through AMA Abuse
- Advisory: Critical Security Updates for Microsoft

🚨 Vulnerability of the Week

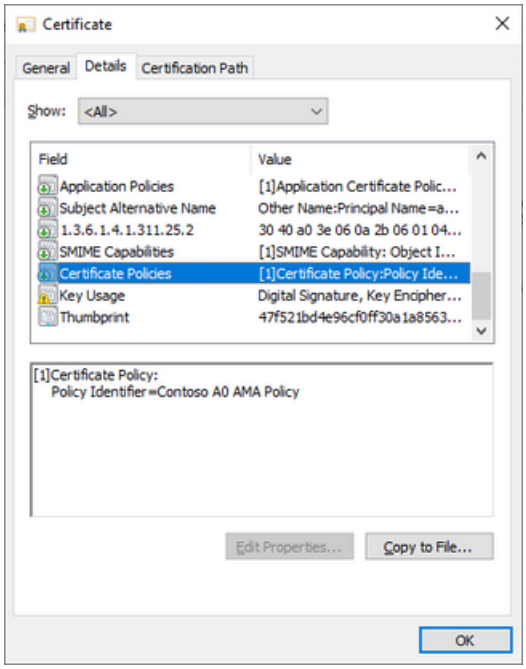
Windows CVE-2024-30078

Microsoft has identified a critical vulnerability in the Wi-Fi driver, designated CVE-2024-30078, with a severity rating of 8.8. This vulnerability has not been publicly disclosed, nor has it been observed in active attacks. However, its exploitation is deemed "less likely" according to Microsoft.

An unauthenticated attacker could exploit this vulnerability by sending a malicious networking packet to an adjacent system using a Wi-Fi networking adapter. Successful exploitation could lead to remote code execution, allowing the attacker to run malware or spyware on the victim's computer without any physical interaction or authentication.

This flaw affects every supported version of Windows and poses a significant risk as it allows remote code execution on nearby Windows PCs via their Wi-Fi connections. This makes it particularly attractive to attackers and security researchers alike.

Art of Detection



https://x.com/m3g9tr0n/status/1802833023622058058

The exploitation of AMA (Active Management Authentication) can lead to severe security risks, including potential forest compromise. This advisory outlines methods to exploit this behavior through both offline (Supply in Request) and online (Build from Active Directory Information) requests. The primary focus is on demonstrating how to inject a Certificate Policy into an issued certificate using an Enterprise Certificate Authority (CA) and templates.

Methods of Exploitation

Offline (Supply in Request)

For offline requests, you can add the Certificate Policies extension in two ways:

1. Include it in the original request as an extension before submitting it to the CA.
2. Add it to a pending request as a Certificate Manager after submitting it to the CA.

Online (Build from Active Directory Information)

For online requests, you can only add the Certificate Policies extension to a pending request. Information other than the public key is ignored in an online request and replaced with data from the user's account in Active Directory and specified templates.

Requirements

- Permissions: The examples assume Enterprise Admin privileges.
- CA Type: These methods apply to Enterprise CA. A Standalone CA can only handle offline requests.
- Tools: A PowerShell module for certificate requests, CertRequestTools, is used for demonstration.

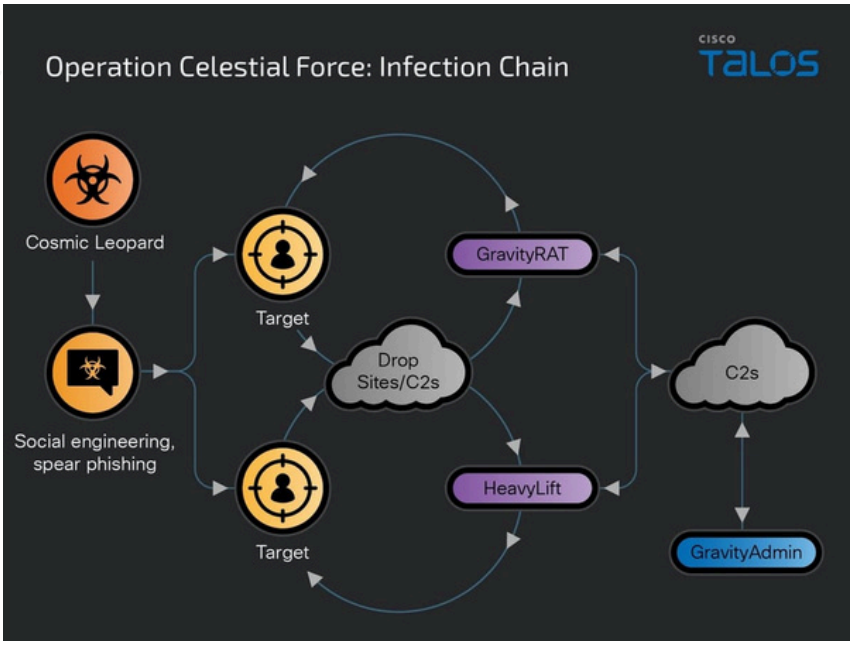
Templates Creation

1. User BFAD Template:
   - Clone the standard User template.
   - Set compatibility to Windows Server 2016 / Windows 10.
   - Name it "User BFAD" for online requests.
   - Set the Provider Category to Key Storage Provider and Algorithm to RSA.
   - Enable CA certificate manager approval.
   - Adjust template security to allow enrollment only for Enterprise Admins and Domain Admins.
   - Optionally remove Encrypting File System and Secure Email EKUs.
2. User SITR Template:
   - Duplicate the User BFAD template.
   - Name it "User SITR" for offline requests.
   - Change the setting to "Supply in the request."

Publish the two templates on your chosen CA.

The abuse of AMA can significantly compromise a forest's security if not properly managed. This advisory highlights the importance of correctly configuring your Public Key Infrastructure (PKI) to prevent unauthorized certificate issuance and policy injection. Always ensure that your CA and templates are securely configured and that only trusted administrators have the necessary privileges to manage certificates.

😈 Malware or Ransomware



https://x.com/virusbtn/status/1802646368789369198

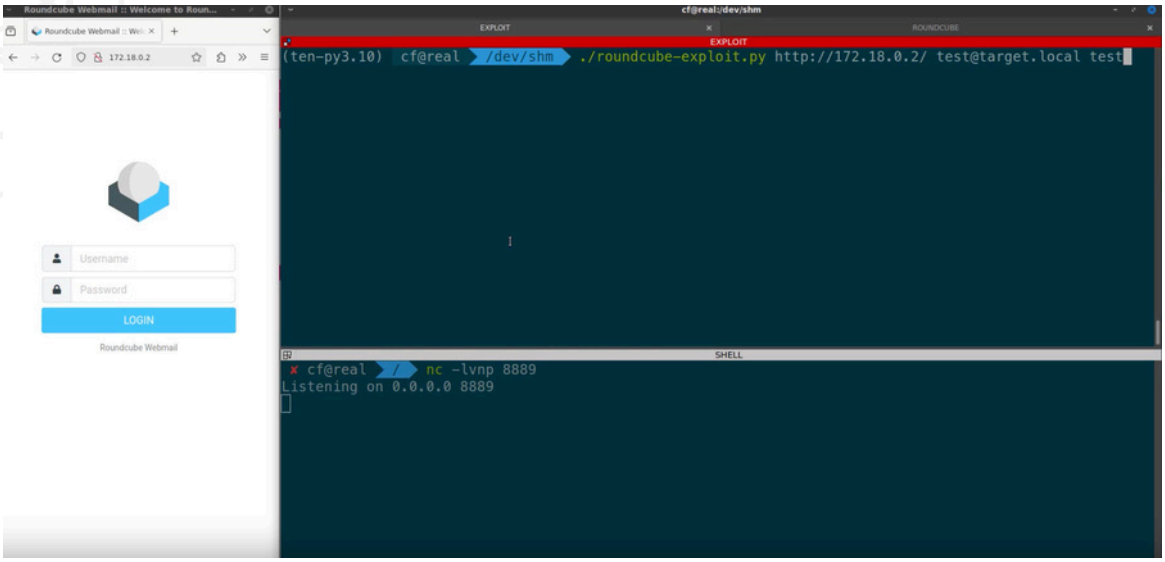
GravityRAT, initially disclosed by Talos in 2018, is a Windows-based remote access trojan (RAT) that has since evolved to target Android devices by 2019. Its development and enhancement over the years have been continuous, with new capabilities being added regularly. This RAT has been primarily used by suspected Pakistani threat actors to target Indian entities and individuals, with no evidence suggesting it is a commodity or open-source malware. This exclusivity points to its likely use by a specific group of threat actors, possibly tied to state-sponsored activities.

Our comprehensive analysis of Operation Celestial Force indicates that GravityRAT has been active since 2016, targeting victims through various means, including malicious websites masquerading as legitimate Android applications. These websites, some of which were registered as recently as January 2024, distribute the malware through download links shared on social media channels. Upon installation, the trojan registers the infected device with a command-and-control (C2) server, concealing its true location using Cloudflare services. GravityRAT's evolving capabilities include sending detailed device information to the C2, reading and uploading SMS data, call logs, specific file formats, and even deleting contacts and logs to cover its tracks.

In parallel, the operation also utilizes an Electron-based malware loader known as HeavyLift. This loader acts as a stage-one malware component, downloading and installing additional malicious implants from the same C2 servers that control GravityRAT. HeavyLift is introduced through executables disguised as legitimate application installers. It conducts preliminary system checks and, depending on the operating system (macOS or Windows), sets specific HTTP User-Agents and collects system information. On macOS, it leverages osascript for privilege escalation, while on Windows, it creates scheduled tasks for persistence.

HeavyLift employs various anti-analysis techniques, including checks for virtual environments and specific keywords associated with virtualization software. If detected, the malware ceases operation to avoid analysis. This sophisticated approach underscores the advanced nature of the threat actors behind these campaigns. Both GravityRAT and HeavyLift highlight the necessity for robust security measures, including up-to-date anti-malware tools, user education on phishing and social engineering tactics, and rigorous monitoring of network traffic for suspicious activities.

1Day



https://x.com/ambionics/status/1802614065979633692

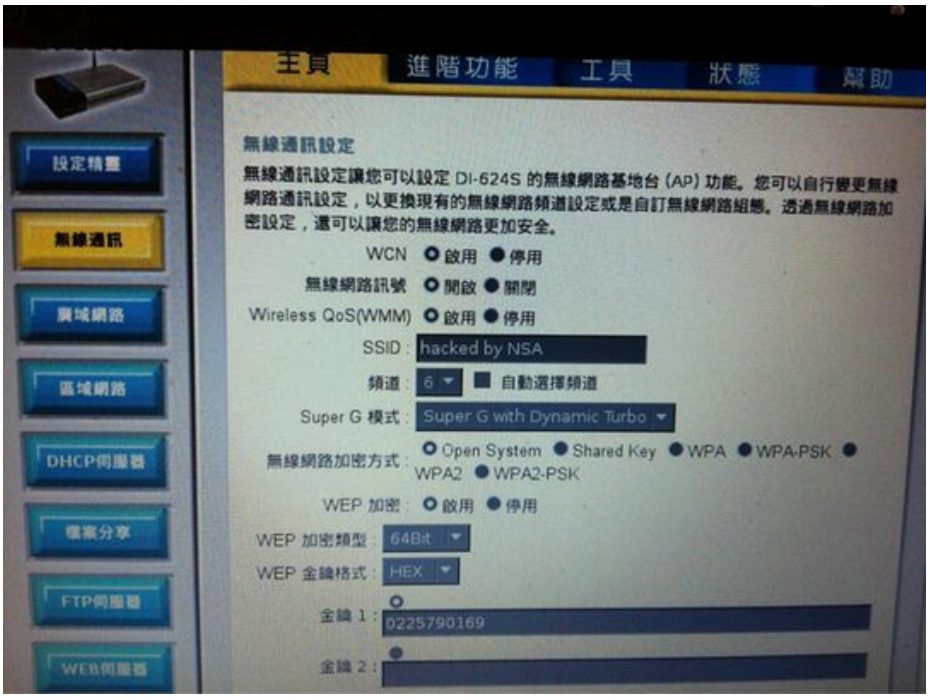
CVE-2024-2961 is a critical vulnerability affecting the iconv() function in PHP, a widely-used programming language for web development. This vulnerability not only impacts iconv() but also potentially its sibling functions, and a popular PHP extension called mbstring. The vulnerability has significant implications for web applications and frameworks that rely on these functions and extensions.

Direct Calls to iconv()
The iconv() function, used for character set conversion, is directly exploitable. This function is essential for many web applications that handle various character encodings.

Sibling Functions
Functions related to iconv(), such as iconv_strrpos(), iconv_substr(), and others, may also be vulnerable. These functions should be reviewed for potential security issues.

mbstring Extension
The mbstring extension, written in C, allows manipulation of strings under various charsets and performs character set conversions. It is widely used in many frameworks and CMSes.
symfony/polyfill-mbstring Project When mbstring is not installed (which requires superuser rights), developers can use the symfony/polyfill-mbstring project. This project mimics the mbstring API using PHP and relies on iconv() for character set conversion. This makes applications using symfony/polyfill-mbstring vulnerable to CVE-2024-2961.

NDay



https://x.com/jedisct1/status/1802674267617640606

Two significant vulnerabilities have been identified in the EAGLE PRO AI and AQUILA PRO AI families of D-Link devices, impacting various models and hardware revisions. Reported by TWCERT in April 2024, these vulnerabilities, CVE-2024-6044 and CVE-2024-6045, allow for LAN-side arbitrary file reading and elevated unauthenticated access respectively. D-Link has verified these vulnerabilities and released fixes through automatic updates. Users can also manually trigger updates via the D-Link Device Mobile applications.
Details of Vulnerabilities
CVE-2024-6044: LAN-Side Arbitrary File Reading

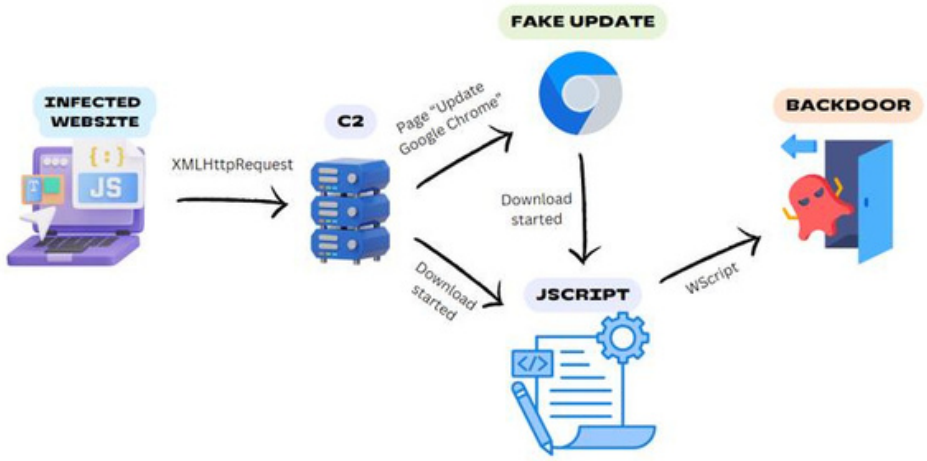
- CVSS Score: 6.5 (Medium)
- CVSS Vector: CVSS:3.1/AV
- CWE: CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CAPEC: CAPEC-126: Path Traversal

This vulnerability allows unauthenticated attackers on the same network to exploit a path traversal issue, enabling them to read arbitrary system files. The improper limitation of pathname handling leads to unauthorized access to sensitive files.
CVE-2024-6045: LAN-Side Unauthenticated Access to Management Features

- CVSS Score: 8.8 (High)
- CVSS Vector: CVSS:3.1/AV
- CWE: CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CAPEC: CAPEC-126: Path Traversal

This vulnerability allows unauthenticated attackers on the same network to enable the device's telnet service by accessing a specific URL. Attackers can then log in using hardcoded credentials obtained from reverse engineering the firmware, gaining elevated access to the device’s management features.

The Topic of the Week



https://x.com/Dinosn/status/1802650078856855748

Cybersecurity researchers have uncovered a malicious campaign leveraging legitimate-but-compromised websites to distribute a Windows backdoor known as BadSpace under the guise of fake browser updates. According to German cybersecurity firm G DATA, the threat actor behind this campaign uses a multi-stage attack chain that includes an infected website, a command-and-control (C2) server, fake browser update prompts, and a JScript downloader to deploy the backdoor onto victims' systems.

The attack begins with a compromised website, often built on platforms such as WordPress, where injected code determines if a user is visiting for the first time. Upon a first-time visit, the injected code collects device information, IP address, user-agent, and location, and transmits this data to a hard-coded domain through an HTTP GET request. If the server detects a new user, it responds by overlaying the webpage with a fake Google Chrome update pop-up window. This pop-up either directly drops the malware or deploys a JavaScript downloader that subsequently installs BadSpace.

Detailed analysis of the C2 servers linked to this campaign reveals connections to SocGholish (also known as FakeUpdates), a well-known JavaScript-based downloader malware. SocGholish shares a similar propagation mechanism, further linking the two campaigns. BadSpace itself is equipped with several sophisticated features: it performs anti-sandbox checks, establishes persistence using scheduled tasks, and is capable of harvesting system information. The malware can also process commands to take screenshots, execute instructions via cmd.exe, read and write files, and delete the scheduled task to evade detection.

This campaign underscores the importance of maintaining robust security practices, especially on websites vulnerable to compromise. Organizations and individuals are advised to keep their web platforms up to date, use security plugins, and regularly scan for vulnerabilities. Users should be cautious of unexpected browser update prompts and verify updates through official channels. Implementing multi-layered security solutions and conducting regular security awareness training can help mitigate the risks posed by threats like BadSpace.

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:
WWW.HADESS.IO

Threat Radar
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.