TLP WHITE: CVE Threat Intelligence Report February 7th 2024

leave a comment »

This threat intelligence report provides an overview of several notable vulnerabilities identified in various software systems and applications. Each vulnerability is presented with its importance, how it works, and the potential larger impacts it may have on affected systems.

CVE-2024-23941 – Group Office Cross-site Scripting Vulnerability

- **Importance:** Medium (CVSS v3.1: 5.4)
- **Overview:** This vulnerability exists in various versions of Group Office and allows remote authenticated attackers to execute arbitrary scripts in the context of a user's web browser session.
- **Impact:** Successful exploitation can lead to session hijacking, redirection to malicious sites, or phishing attacks, potentially compromising sensitive information.

CVE-2023-30999 – IBM Security Access Manager Denial of Service

- **Importance:** High (CVSS v3.1: 7.5)
- **Overview:** This issue affects IBM Security Verify Access appliances and containers, allowing attackers to cause a denial of service through uncontrolled resource consumption.
- **Impact:** An attacker can disrupt service for legitimate users, affecting the availability of critical security management functions.

CVE-2024-1197 – SourceCodester Testimonial Page Manager Critical Vulnerability

- **Importance:** Critical (CVSS v3.1: 9.8)
- **Overview:** Affects the deletion functionality of testimonials, leading to unauthorized actions without proper validation.
- **Impact:** This critical vulnerability can lead to unauthorized access, data manipulation, or complete system compromise due to insufficient input validation.

CVE-2024-24161 – MRCMS Arbitrary File Read Vulnerability

- **Importance:** High (CVSS v3.1: 7.5)
- **Overview:** This vulnerability allows attackers to read arbitrary files on the server due to insufficient filtering of the path parameter.
- **Impact:** Could lead to sensitive information disclosure, aiding attackers in further exploitation efforts.

CVE-2024-24470 – Flusity-CMS Cross Site Request Forgery

- **Importance:** High (CVSS v3.1: 8.8)
- **Overview:** Enables attackers to execute unauthorized commands on behalf of authenticated users.
- **Impact:** This vulnerability can lead to unauthorized changes in content or configurations, potentially compromising the integrity of the site.

CVE-2024-24029 – JFinalCMS SQL Injection

- **Importance:** Critical (CVSS v3.1: 9.8)
- **Overview:** A SQL injection vulnerability that allows attackers to execute arbitrary SQL commands through the content data interface.
- **Impact:** Attackers can access or modify data, escalate privileges, or attack underlying databases, leading to significant data breaches.

CVE-2024-24160 – MRCMS Cross-Site Scripting (XSS) Vulnerability

- **Importance:** Medium (CVSS v3.1: 5.4)
- **Overview:** Similar to CVE-2024-23941, allows execution of arbitrary scripts due to insufficient input sanitization.
- **Impact:** Raises concerns for user data security and integrity of sessions, similar to other XSS vulnerabilities.

CVE-2024-1196 – SourceCodester Testimonial Page Manager Problematic Vulnerability

- **Importance:** Medium (CVSS v3.1: 6.1)
- **Overview:** Pertains to handling of HTTP POST requests, leading to unspecified vulnerability.
- **Impact:** While less detailed, such vulnerabilities typically allow unauthorized actions or data exposure.

Additional CVEs of Note:

- **CVE-2023-6676, CVE-2023-0686, CVE-2024-23745:** These critical vulnerabilities, including CSRF and Dirty NIB attacks, highlight the diverse nature of threats, from web-based exploits to application-specific vulnerabilities, all leading to significant impacts such as unauthorized command execution, data breaches, or system compromise.
- **CVE-2023 Series (QNAP Vulnerabilities):** These vulnerabilities in QNAP systems underscore the risks to network storage devices, including DoS attacks, code execution, and command injection, affecting confidentiality, integrity, and availability of data.

HIGH Known Exploited CVE’s 2023-2024

CVE-2023-4762 – Google Chrome Type Confusion Vulnerability

- **Severity:** High
- **CVSS Score:** 8.8
- **Description:** A type confusion flaw in the V8 JavaScript engine in Google Chrome allowed remote attackers to execute arbitrary code via a specially crafted HTML page.
- **Impact:** This vulnerability enables attackers to compromise systems running an outdated version of Chrome by executing arbitrary code under the privileges of the user running the browser.

CVE-2024-21893 – Ivanti Connect Secure Server-Side Request Forgery

- **Severity:** High
- **CVSS Score:** 8.2
- **Description:** A server-side request forgery (SSRF) vulnerability in Ivanti Connect Secure's SAML component permits attackers to access restricted resources without authentication.
- **Impact:** The exploitation of this vulnerability could lead to unauthorized access to sensitive data or internal systems, potentially breaching the security perimeter of affected organizations.

CVE-2022-48618 – Apple Pointer Authentication Bypass

- **Severity:** High
- **CVSS Score:** 7.8
- **Description:** A vulnerability in various Apple operating systems that allows attackers with arbitrary read and write capability to bypass Pointer Authentication.
- **Impact:** This issue may enable attackers to execute arbitrary code with kernel privileges, significantly compromising the security of affected devices.

CVE-2023-22527 – Confluence Data Center and Server Template Injection

- **Severity:** Critical
- **CVSS Score:** 10.0
- **Description:** An unauthenticated template injection vulnerability in older versions of Confluence allows for remote code execution (RCE) on affected instances.
- **Impact:** This critical vulnerability can lead to complete system compromise, enabling attackers to gain unauthorized access and control over affected systems.

CVE-2024-23222 – Apple Type Confusion Vulnerability

- **Severity:** High
- **CVSS Score:** 8.8

- **Description:** A type confusion issue in various Apple software was fixed, which could allow for arbitrary code execution through malicious web content.
- **Impact:** Successful exploitation could compromise the security of affected devices, potentially leading to data theft, system access, or further malicious activities.

CVE-2023-34048 – VMware vCenter Server Out-of-Bounds Write

- **Severity:** Critical
- **CVSS Score:** 9.8
- **Description:** A vulnerability in the DCERPC protocol implementation in vCenter Server that could allow remote code execution.
- **Impact:** This vulnerability poses a significant risk as it could enable attackers to take control of the affected systems, compromising the security and integrity of enterprise virtual environments.

CVE-2023-35082 – Ivanti EPMM Authentication Bypass

- **Severity:** Critical
- **CVSS Score:** 10.0
- **Description:** An authentication bypass vulnerability in Ivanti EPMM allows unauthorized access to restricted functionality or resources without proper authentication.
- **Impact:** The exploitation of this vulnerability could allow attackers to bypass security mechanisms, gaining unauthorized access to sensitive data or functionalities.

CVE-2024-0519 – Google Chrome Out of Bounds Memory Access

- **Severity:** High
- **CVSS Score:** 8.8
- **Description:** A vulnerability in the V8 engine of Google Chrome that could allow remote attackers to exploit heap corruption via a crafted HTML page.
- **Impact:** This vulnerability could lead to system compromise through the execution of arbitrary code or crashing the browser, posing significant risks to data security and system integrity.

Additional Notable CVEs:

- **CVE-2023-6549 and CVE-2023-6548:** These vulnerabilities in NetScaler ADC and Gateway highlight the risk of denial of service and remote code execution due to improper memory operations and code injection vulnerabilities.
- **CVE-2018-15133 (Laravel Framework RCE):** Demonstrates the long-term implications of serialized data manipulation vulnerabilities in web applications.

- **CVE-2024-21887 (Ivanti Command Injection):** A command injection vulnerability allowing authenticated administrators to execute arbitrary commands, showcasing risks even from authenticated users.
- **CVE-2023-29357 (Microsoft SharePoint EoP):** An elevation of privilege vulnerability in SharePoint Server, underscoring the importance of securing enterprise collaboration platforms.

The vulnerabilities listed in this report underscore the diversity and severity of threats facing software and systems across different platforms and applications. They highlight the necessity for ongoing vigilance, timely updates, and comprehensive security measures to protect against potential exploitation. Addressing these vulnerabilities promptly is critical to safeguarding sensitive information and maintaining the integrity and availability of affected systems and networks.