aruba.it

Vulnerability Assessment Report

Table of Contents

Assessment Scope

Target Definition	www.dominioprovasicurezzawp.it

Executive Summary

This vulnerability assessment report presents the findings of a comprehensive security evaluation conducted on the target system. The assessment identified **13 vulnerabilities** across various severity levels, ranging from informational findings to critical security issues that require immediate attention.

Key Findings:
• **Critical:** 1 vulnerabilities requiring immediate remediation
• **High:** 2 vulnerabilities requiring urgent attention
• **Medium:** 10 vulnerabilities requiring important consideration
• **Low:** 0 vulnerabilities with minimal impact
• **Informational:** 0 findings for security awareness

Assessment Methodology:
This vulnerability assessment was conducted using industry-standard security testing methodologies and tools. The evaluation included automated vulnerability scanning, manual security testing, and comprehensive analysis of identified security issues. Each vulnerability was assessed for its potential impact, exploitability, and business risk to provide actionable remediation recommendations.

Immediate Actions Required:
Organizations should prioritize remediation efforts based on severity levels, starting with critical and high-severity vulnerabilities. A comprehensive security program should include regular vulnerability assessments, patch management processes, and ongoing security monitoring to maintain a strong security posture.

Security Risk Assessment Framework

This framework provides standardized severity classifications and response guidelines for security vulnerabilities based on industry best practices and risk assessment methodologies.

Severity Level	Risk Description
Critical	Vulnerabilities that pose an immediate and severe threat to the system
High	Vulnerabilities that could lead to significant security breaches
Medium	Vulnerabilities that could be exploited but with limited impact
Low	Vulnerabilities with minimal security impact
Info	Informational findings that may be useful for security awareness

Vulnerability Summary Table

Title	Severity	CVSS Score
Modern Events Calendar Lite <= 6.1.4 - Unauthenticated Blind SQL Injection via Time Parameter	Critical	9.8
Modern Events Calendar <= 7.11.0 - Authenticated (Subscriber+) Arbitrary File Upload	High	8.8
Modern Events Calendar <= 7.12.1 - Authenticated (Subscriber+) Server Side Request Forgery	High	8.5
WordPress XML-RPC System Method Listing	Medium	5.3
Modern Events Calendar Lite <= 6.1.0 - Reflected Cross-Site Scripting via Current_month_divider Parameter	Medium	6.1
Modern Events Calendar Lite <= 6.1.6 - Subscriber+ Category Add Leading to Stored Cross-Site Scripting	Medium	5.4
Modern Events Calendar Lite <= 6.3.0 - Unauthenticated SQL Injection	Medium	5.9
Modern Events Calendar Lite <= 6.3.0 - Stored Cross-Site Scripting	Medium	6.4
Modern Events Calendar Lite <= 6.5.1 - Authenticated (Admin+) Stored Cross-Site Scripting	Medium	5.5
Modern Events Calendar Lite <= 6.2.9 - Authenticated (Contributor+) Cross-Site Scripting	Medium	6.4
Modern Events Calendar Lite < 6.10.5 - Authenticated (Admin+) Stored Cross-Site Scripting	Medium	4.4
Modern Events Calendar Lite < 7.1.0 - Authenticated (Admin+) Stored Cross-Site Scripting	Medium	4.4

Modern Events Calendar <= 7.21.9 - Information Exposure	Medium	5.3

Detailed Vulnerability Information

Modern Events Calendar Lite <= 6.1.4 - Unauthenticated Blind SQL Injection via Time Parameter

Severity	Critical
CVSS Score	9.8
CVE ID	CVE-2021-24946
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description
The Modern Events Calendar Lite WordPress plugin before 6.1.5 does not sanitise and escape the time parameter before using it in a SQL statement in the mec_load_single_page AJAX action, available to unauthenticated users, leading to an unauthenticated SQL injection issue

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24946

Modern Events Calendar <= 7.11.0 - Authenticated (Subscriber+) Arbitrary File Upload

Severity	High
CVSS Score	8.8
CVE ID	CVE-2024-5441
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Description
The Modern Events Calendar plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the set_featured_image function in all versions up to, and including, 7.11.0.

Impact
This makes it possible for authenticated attackers, with subscriber access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. The plugin allows administrators (via its settings) to extend the ability to submit events to unauthenticated users, which would allow unauthenticated attackers to exploit this vulnerability.

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-5441

Modern Events Calendar <= 7.12.1 - Authenticated (Subscriber+) Server Side Request Forgery

Severity	High
CVSS Score	8.5
CVE ID	CVE-2024-6522
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N

Description
The Modern Events Calendar plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 7.12.1 via the 'mec_fes_form' AJAX function.

Impact
This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-6522

WordPress XML-RPC System Method Listing

Severity	Medium
CVSS Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description
XML-RPC interface is enabled and allows enumeration of available system methods, potentially revealing functionality that can be exploited.

Impact
An attacker could discover available XML-RPC methods and functionality, which may be leveraged for brute force attacks, denial of service, or other malicious activities against the WordPress installation.

Mitigation
Disable XML-RPC if not required. If needed, implement proper authentication and rate limiting. Use security plugins to restrict XML-RPC access and monitor for suspicious XML-RPC activity.

Steps to Reproduce

```
curl -X 'POST' \
-d '<?xml version="1.0" encoding="utf-8"?><methodCall><methodName>system.
listMethods</methodName><params></params></methodCall>' \
-H 'Accept: */*' -H 'Accept-Language: en' \
-H 'User-Agent: Mozilla/5.0 (Knoppix; Linux i686; rv:127.0)
Gecko/20100101 Firefox/127.0'
'https://www.dominioprovasicurezzawp.it/xmlrpc.php'
```

Modern Events Calendar Lite <= 6.1.0 - Reflected Cross-Site Scripting via Current_month_divider Parameter

Severity	Medium
CVSS Score	6.1
CVE ID	CVE-2021-24925
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description
The Modern Events Calendar Lite WordPress plugin before 6.1.5 does not sanitise and escape the current_month_divider parameter of its mec_list_load_more AJAX call (available to both unauthenticated and authenticated users) before outputting it back in the response, leading to a Reflected Cross-Site Scripting issue

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24925

Modern Events Calendar Lite <= 6.1.6 - Subscriber+ Category Add Leading to Stored Cross-Site Scripting

Severity	Medium
CVSS Score	5.4
CVE ID	CVE-2021-25046
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

Description
The Modern Events Calendar Lite WordPress plugin before 6.2.0 alloed any logged-in user, even a subscriber user, may add a category whose parameters are incorrectly escaped in the admin panel, leading to stored XSS.

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25046

Modern Events Calendar Lite <= 6.3.0 - Unauthenticated SQL Injection

Severity	Medium
CVSS Score	5.9
CVE ID	CVE-2021-4458
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Description
The Modern Events Calendar Lite plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter of the 'wp_ajax_mec_load_single_page' AJAX action in all versions up to, and including, 6.3.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query.

Impact
This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is only exploitable on sites with addslashes disabled.

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4458

Modern Events Calendar Lite <= 6.3.0 - Stored Cross-Site Scripting

Severity	Medium
CVSS Score	6.4
CVE ID	CVE-2022-0364
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

Description
The Modern Events Calendar Lite WordPress plugin before 6.4.0 does not sanitize and escape some of the Hourly Schedule parameters which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0364

Modern Events Calendar Lite <= 6.5.1 - Authenticated (Admin+) Stored Cross-Site Scripting

Severity	Medium
CVSS Score	5.5
CVE ID	CVE-2022-27848
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N

Description
The Modern Events Calendar Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 6.5.1 due to insufficient input sanitization and output escaping.

Impact
This makes it possible for authenticated attackers with administrative privileges to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27848

Modern Events Calendar Lite <= 6.2.9 - Authenticated (Contributor+) Cross-Site Scripting

Severity	Medium
CVSS Score	6.4
CVE ID	CVE-2022-30533
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

Description
The Modern Events Calendar Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an unknown parameter in versions up to, and including, 6.2.9 due to insufficient input sanitization and output escaping.

Impact
This makes it possible for authenticated attackers with contributor-level permissions and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30533

Modern Events Calendar Lite < 6.10.5 - Authenticated (Admin+) Stored Cross-Site Scripting

Severity	Medium
CVSS Score	4.4
CVE ID	CVE-2023-1400
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N

Description
The Modern Events Calendar lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Google API key and Calendar ID in versions up to, and including, 6.10.5 due to insufficient input sanitization and output escaping.

Impact
This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1400

Modern Events Calendar Lite < 7.1.0 - Authenticated (Admin+) Stored Cross-Site Scripting

Severity	Medium
CVSS Score	4.4
CVE ID	CVE-2023-4021
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N

Description
The Modern Events Calendar lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Google API key and Calendar ID in versions up to, but not including, 7.1.0 due to insufficient input sanitization and output escaping.

Impact
This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4021

Modern Events Calendar <= 7.21.9 - Information Exposure

Severity	Medium
CVSS Score	5.3
CVE ID	CVE-2025-5733
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description
The Modern Events Calendar Lite plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 7.21.9. This is due improper or insufficient validation of the id property when exporting calendars.

Impact
This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.

Mitigation
Update the modern-events-calendar-lite plugin to the latest version available

References
• https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-5733

aruba.it