



Site Search

[Full Disclosure](#) mailing list archives[← By Date →](#) [← By Thread →](#)

List Archive Search



Admin-only local file inclusion and arbitrary code execution in Subscribe to Comments 2.1.2 (WordPress plugin)

From: dxw Security <security () dxw com>
Date: Tue, 14 Jul 2015 11:19:40 +0000

Details

=====
Software: Subscribe to Comments
Version: 2.1.2
Homepage: <http://wordpress.org/plugins/subscribe-to-comments/>
Advisory report:
<https://security.dxw.com/advisories/admin-only-local-file-inclusion-and-arbitrary-code-execution-in-subscribe-to-comments-2-1-2/>
CVE: Awaiting assignment
CVSS: 8 (High; AV:N/AC:L/Au:S/C:C/I:P/A:P)

Description

=====
Admin-only local file inclusion and arbitrary code execution in Subscribe to Comments 2.1.2

Vulnerability

=====
Administrators can perform Local File include attacks, which is a privilege escalation on systems where the administrator doesn't have control over the server.
If administrators can upload PHP files (or any file which can contain "<?php ..."), they can also perform arbitrary code execution by the same method.

Proof of concept

=====
<http://localhost/wp-admin/options-general.php?page=stc-options>
Set "Path to header" to "/etc/passwd"
Check "Use custom style for Subscription Manager"
"Update Options"
<https://localhost/?wp-subscription-manager=1>

Mitigations

=====
Upgrade to version 2.3 or later

Disclosure policy

=====

dxw believes in responsible disclosure. Your attention is drawn to our disclosure policy:

<https://security.dxw.com/disclosure/>

Please contact us on security () dxw com to acknowledge this report if you received it via a third party (for example, plugins () wordpress org) as they generally cannot communicate with us on your behalf.

This vulnerability will be published if we do not receive a response to this report with 14 days.

Timeline

=====

2013-08-07: Discovered

2015-07-13: Reported to vendor by email

2015-07-13: Requested CVE

2015-07-14: Vendor responded confirming fixed in version 2.3

2015-07-14: Published

Discovered by dxw:

=====

Tom Adams

Please visit security.dxw.com for more information.

Sent through the Full Disclosure mailing list

<https://nmap.org/mailman/listinfo/fulldisclosure>

Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[← By Date →](#) [← By Thread →](#)

Current thread:

Admin-only local file inclusion and arbitrary code execution in Subscribe to Comments 2.1.2 (WordPress plugin) dxw Security (Jul 14)

Site Search



Nmap Security Scanner

Npcap packet capture

Security Lists

Security Tools

About

Ref Guide

User's Guide

Nmap Announce

Vuln scanners

About/Contact

Install Guide

API docs

Nmap Dev

Password audit

Privacy

Docs

Download

Full Disclosure

Web scanners

Advertising

Download

Npcap OEM

Open Source Security

Wireless

Nmap Public Source License

Nmap OEM

BreachExchange

Exploitation



