dxw
advisories

Advisory:

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

Vulnerability

Last revised: July 13, 2015

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.

Current state: Fixed

CVSS Summary

Score	**8 High**
Vector	Network
Complexity	Low
Authentication	Single
Confidentiality	Complete
Integrity	Partial
Availability	Partial

You can read more about CVSS base scores on Wikipedia or in the CVSS specification.

Discovered by:
Mallory Adams and dxwsupport

Advisory ID:
dxw-1970-484

CVE:
Awaiting assignment

Component/package:
Subscribe to Comments

Homepage:
Subscribe to Comments

Version:
2.1.2

Proof of concept

1. http://localhost/wp-admin/options-general.php?page=stc-options
2. Set “Path to header” to “/etc/passwd”
3. Check “Use custom style for Subscription Manager”
4. “Update Options”
5. https://localhost/?wp-subscription-manager=1

Advisory 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

Mitigation/further actions

Upgrade to version 2.3 or later