OpenVas Vulnerability Report

HackerTarget.com hosts a suite of **trusted open source** vulnerability scanners. Secure your Attack Surface with our vulnerability discovery and network intelligence solutions.

This report was autogenerated using the open source OpenVAS Vulnerability Scanner.

Table of Contents

Summary

Scan started: **Wed Feb 13 04:07:18 2019 UTC**
Scan ended: Wed Feb 13 04:19:08 2019 UTC

1	7	2
HIGH	MEDIUM	LOW

Any **HIGH** and **MEDIUM** severity vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.

Host Summary

Host	Start	End	High	Medium	Low	Log
192.168.1.222	Feb 13, 04:07	Feb 13, 04:19	1	7	2	0
Total: 1			1	7	2	0

Vulnerability Summary

Severity	Description	CVSS	Count
High	Webmin <= 1.900 RCE Vulnerability	9.0	1
Medium	WordPress NextGEN Gallery Plugin < 2.1.57 Local File Inclusion Vulnerability	6.0	2
Medium	WordPress User IDs and User Names Disclosure	5.8	1
Medium	Webmin 1.880 Information Disclosure Vulnerability	5.0	1
Medium	Cleartext Transmission of Sensitive Information via HTTP	4.8	1
Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili...	4.0	2
Low	WordPress Yoast SEO Plugin XSS Vulnerability	3.5	2

Results by Host

Host 192.168.1.222

Host scan started: Wed Feb 13 04:07:34 2019 UTC

Port Summary for Host 192.168.1.222

Service (Port)	Severity
12321/tcp	High
443/tcp	Medium
80/tcp	Medium

Security Issues for Host 192.168.1.222

High (CVSS: 9.0) 12321/tcp
NVT: Webmin <= 1.900 RCE Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.141897)

Product detection result: cpe:/a:webmin:webmin:1.780 by Webmin / Usermin Detection (OID: 1.3.6.1.4.1.25623.1.0.10757)

Summary

Webmin is prone to an authenticate remote code execution vulnerability.

Vulnerability Detection Result

Installed version: 1.780
Fixed version: None

Solution

Solution type: NoneAvailable

No known solution is available as of 21st January, 2019. Information regarding this issue will be updated once solution details are available.

Affected Software/OS

Webmin version 1.900 and probably prior.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: Webmin <= 1.900 RCE Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.141897)

Version used: $Revision: 13183 $

Product Detection Result

Product: cpe:/a:webmin:webmin:1.780
Method: Webmin / Usermin Detection (OID: 1.3.6.1.4.1.25623.1.0.10757)

References

Other: https://www.exploit-db.com/exploits/46201

Medium (CVSS: 6.0) 443/tcp
NVT: WordPress NextGEN Gallery Plugin < 2.1.57 Local File Inclusion Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.112326)

Product detection result: cpe:/a:wordpress:wordpress:4.4.17 by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary

The Imagely NextGen Gallery plugin for Wordpress may execute code from an uploaded malicious file.

Vulnerability Detection Result

Installed version: 2.1.31
Fixed version: 2.1.57

Impact

An authenticated user may be able to read arbitrary files on the server or execute code on the server by including a malicious local file in a formatted server request.

Solution

Solution type: VendorFix

Update to version 2.1.57 or later.

Affected Software/OS

WordPress NextGEN Gallery plugin before 2.1.57.

Vulnerability Insight

The Imagely NextGen Gallery plugin for Wordpress does not properly validate user input in the cssfile parameter of a HTTP POST request, which may allow an authenticated user to read arbitrary files from the server, or execute arbitrary code on the server in some circumstances (dependent on server configuration).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: WordPress NextGEN Gallery Plugin < 2.1.57 Local File Inclusion Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.112326)

Version used: $Revision: 11317 $

Product Detection Result

Product: cpe:/a:wordpress:wordpress:4.4.17
Method: WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

References

CVE: CVE-2016-6565
BID: 94356
Other: https://wordpress.org/plugins/nextgen-gallery/#developers
https://www.kb.cert.org/vuls/id/346175

Medium (CVSS: 6.0) 80/tcp
NVT: WordPress NextGEN Gallery Plugin < 2.1.57 Local File Inclusion Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.112326)

Product detection result: cpe:/a:wordpress:wordpress:4.4.17 by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary

The Imagely NextGen Gallery plugin for Wordpress may execute code from an uploaded malicious file.

Vulnerability Detection Result

Installed version: 2.1.31
Fixed version: 2.1.57

Impact

An authenticated user may be able to read arbitrary files on the server or execute code on the server by including a malicious local file in a formatted server request.

Solution

Solution type: VendorFix

Update to version 2.1.57 or later.

Affected Software/OS

WordPress NextGEN Gallery plugin before 2.1.57.

Vulnerability Insight

The Imagely NextGen Gallery plugin for Wordpress does not properly validate user input in the cssfile parameter of a HTTP POST request, which may allow an authenticated user to read arbitrary files from the server, or execute arbitrary code on the server in some circumstances (dependent on server configuration).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: WordPress NextGEN Gallery Plugin < 2.1.57 Local File Inclusion Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.112326)

Version used: $Revision: 11317 $

Product Detection Result

Product: cpe:/a:wordpress:wordpress:4.4.17
Method: WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

References

CVE:	CVE-2016-6565
BID:	94356
Other:	https://wordpress.org/plugins/nextgen-gallery/#developers
	https://www.kb.cert.org/vuls/id/346175

Medium (CVSS: 5.8) 80/tcp
NVT: WordPress User IDs and User Names Disclosure (OID: 1.3.6.1.4.1.25623.1.0.103222)

Product detection result: cpe:/a:wordpress:wordpress:4.4.17 by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary

WordPress platforms use a parameter called `author'. This parameter accepts integer values and represents the `User ID' of users in the web site. For example: http://www.example.com/?author=1

The problems found are: 1. User ID values are generated consecutively. 2. When a valid User ID is found, WordPress redirects to a web page with the name of the author.

These problems trigger the following attack vectors: 1. The query response discloses whether the User ID is enabled. 2. The query response leaks (by redirection) the User Name corresponding with that User ID.

Vulnerability Detection Result

The following user names were revealed in id range 1-25.

Discovered username 'admin' with id '1'

Solution

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Vulnerability Detection Method

Details: WordPress User IDs and User Names Disclosure (OID: 1.3.6.1.4.1.25623.1.0.103222)

Version used: $Revision: 11997 $

Product Detection Result

Product: cpe:/a:wordpress:wordpress:4.4.17
Method: WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

References

Other: http://www.talsoft.com.ar/index.php/research/security-advisories/wordpress-user-id-and-user-name-disclosure

Medium (CVSS: 5.0) 12321/tcp
NVT: Webmin 1.880 Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.113135)

Product detection result: cpe:/a:webmin:webmin:1.780 by Webmin / Usermin Detection (OID: 1.3.6.1.4.1.25623.1.0.10757)

Summary

Webmin is prone to an information disclosure vulnerability that allows non-privileged users to access arbitrary files.

Vulnerability Detection Result

Installed version: 1.780
Fixed version: Please see the solution tag for an available Mitigation

Impact

Successful exploitation would allow an attacker to access any file on the system, ranging from sensitive documents to administrator passwords.

Solution

Solution type: Mitigation

No patch is available as of 15th March, 2018. As a mitigation technique, the setting 'Can view any file as a log file' can be disabled, effectively stopping a user from exploiting this vulnerability.

Affected Software/OS

Webmin through version 1.880

Vulnerability Insight

An issue was discovered in Webmin when the default Yes setting of 'Can view any file as a log file' is enabled. As a result of weak default configuration settings, limited users have full access rights to the underlying Unix system files, allowing the user to read sensitive data from the local system (using Local File Include) such as the '/etc/shadow' file via a 'GET /syslog/save_log.cgi?view=1&file=/etc/shadow' request.

Vulnerability Detection Method

The script checks if a vulnerable version is present on the target host.

Details: Webmin 1.880 Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.113135)

Version used: $Revision: 12116 $

Product Detection Result

Product: cpe:/a:webmin:webmin:1.780
Method: Webmin / Usermin Detection (OID: 1.3.6.1.4.1.25623.1.0.10757)

References

CVE: CVE-2018-8712
Other: https://www.7elements.co.uk/resources/technical-advisories/webmin-1-840-1-880-unrestricted-access-arbitrary-files-using-local-file-include/
http://www.webmin.com/changes.html

Medium (CVSS: 4.8) 80/tcp
NVT: Cleartext Transmission of Sensitive Information via HTTP (OID: 1.3.6.1.4.1.25623.1.0.108440)

Summary

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

The following input fields where identified (URL:input name):

http://192.168.1.222/wp-login.php:pwd

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution

Solution type: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)

- HTTP Forms (e.g. Login) with input field of type 'password'

Details: Cleartext Transmission of Sensitive Information via HTTP (OID: 1.3.6.1.4.1.25623.1.0.108440)

Version used: $Revision: 10726 $

References

Other: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management
https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 4.0) 12321/tcp
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

Server Temporary Key Size: 1024 bits

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method

Checks the DHE temporary public key size.

Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: $Revision: 12865 $

References

Other: https://weakdh.org/
https://weakdh.org/sysadmin.html

Medium (CVSS: 4.0) 443/tcp
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

Server Temporary Key Size: 1024 bits

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method

Checks the DHE temporary public key size.

Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: $Revision: 12865 $

References

Other: https://weakdh.org/
https://weakdh.org/sysadmin.html

Low (CVSS: 3.5) 443/tcp
NVT: WordPress Yoast SEO Plugin XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.112127)

Product detection result: cpe:/a:wordpress:wordpress:4.4.17 by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary

A cross-site scripting (XSS) vulnerability in admin/google_search_console/class-gsc-table.php in the Yoast SEO plugin for WordPress allows remote attackers to inject arbitrary web script or HTML.

Vulnerability Detection Result

Installed version: 3.1.2
Fixed version: 5.8.0

Solution

Solution type: VendorFix

Update to version 5.8.0 or later.

Affected Software/OS

WordPress Yoast SEO plugin before version 5.8.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: WordPress Yoast SEO Plugin XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.112127)

Version used: $Revision: 12106 $

Product Detection Result

Product: cpe:/a:wordpress:wordpress:4.4.17
Method: WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

References

CVE: CVE-2017-16842
Other: https://wordpress.org/plugins/wordpress-seo/#developers
https://plugins.trac.wordpress.org/changeset/1766831/wordpress-seo/trunk/admin/google_search_console/class-gsc-table.php

Low (CVSS: 3.5) 80/tcp
NVT: WordPress Yoast SEO Plugin XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.112127)

Product detection result: cpe:/a:wordpress:wordpress:4.4.17 by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary

A cross-site scripting (XSS) vulnerability in admin/google_search_console/class-gsc-table.php in the Yoast SEO plugin for WordPress allows remote attackers to inject arbitrary web script or HTML.

Vulnerability Detection Result

Installed version: 3.1.2
Fixed version: 5.8.0

Solution

Solution type: VendorFix

Update to version 5.8.0 or later.

Affected Software/OS

WordPress Yoast SEO plugin before version 5.8.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: WordPress Yoast SEO Plugin XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.112127)

Version used: $Revision: 12106 $

Product Detection Result

Product: cpe:/a:wordpress:wordpress:4.4.17
Method: WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

References

CVE: CVE-2017-16842
Other: https://wordpress.org/plugins/wordpress-seo/#developers
https://plugins.trac.wordpress.org/changeset/1766831/wordpress-seo/trunk/admin/google_search_console/class-gsc-table.php