OpenVas Vulnerability Report

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

CONFIDENTIAL - This report contains sensitive information and should be stored in a secure location

Table of Contents

Summary

Scan started: **Wed Feb 13 04:26:48 2019 UTC**
Scan ended: Wed Feb 13 04:41:16 2019 UTC

3	**4**	**0**
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
192.168.1.211	Feb 13, 04:27	Feb 13, 04:41	3	4	0	0
Total: 1			3	4	0	0

Vulnerability Summary

Severity	Description	CVSS	Count
High	Webmin <= 1.900 RCE Vulnerability	9.0	1
High	HTTP Brute Force Logins With Default Credentials Reporting	9.0	2
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

Results by Host

Host 192.168.1.211

Host scan started: Wed Feb 13 04:27:04 2019 UTC

Port Summary for Host 192.168.1.211

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

Security Issues for Host 192.168.1.211

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

High (CVSS: 9.0) 443/tcp
NVT: HTTP Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103240)

Summary

It was possible to login into the remote Web Application using default credentials.

As the NVT 'HTTP Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

It was possible to login with the following credentials <Url>:<User>:<Password>:<HTTP status code>

```
 https://192.168.1.211/manager/html:MAIL:MPE:HTTP/1.1 404 Not Found
 https://192.168.1.211/manager/html:PFCUser:240653C9467E45:HTTP/1.1 404 Not Found
 https://192.168.1.211/manager/html:admin:1234:HTTP/1.1 404 Not Found
 https://192.168.1.211/manager/status:operator:operator:HTTP/1.1 404 Not Found
 https://192.168.1.211/manager/status:public::HTTP/1.1 404 Not Found
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Try to login with a number of known default credentials via HTTP Basic Auth.

Details: HTTP Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103240)

Version used: $Revision: 11663 $

High (CVSS: 9.0) 80/tcp
NVT: HTTP Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103240)

Summary

It was possible to login into the remote Web Application using default credentials.

As the NVT 'HTTP Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

It was possible to login with the following credentials <Url>:<User>:<Password>:<HTTP status code>

```
 http://192.168.1.211/manager/html:cellit:cellit:HTTP/1.1 404 Not Found
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Try to login with a number of known default credentials via HTTP Basic Auth.

Details: HTTP Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103240)

Version used: $Revision: 11663 $

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 URLs requires Basic Authentication (URL:realm name):

```
 http://192.168.1.211/host-manager/html:"Tomcat Host Manager Application"
 http://192.168.1.211/manager/html:"Tomcat Manager Application"
 http://192.168.1.211/manager/status:"Tomcat Manager Application"
```

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

This file was automatically generated.