AttackerKB sunset on August 18. Read our blog.

ATTACKER VALUE
VERY HIGH
(9 users assessed)

EXPLOITABILITY
VERY HIGH
(9 users assessed)

42

USER INTERACTION
Unknown

Webmin password_cha

Disclosure Date: August 16, 2019 · (Last upda

CVE-2019-15107

Exploited in the Wild

Reported by gdft2112 and 1 more...
View Source Details

Report As Exploited in the Wild

Quick Cookie Notification

This site uses cookies for anonymized analytics to improve the site.

Rapid7 will never sell the data collected on this site.

I AGREE, LET'S GO!

View our Cookie Policy for full details

Watch This Topic

Watch this topic to be notified when new information, assessments, and comments are added

MITRE ATT&CK

Log in to add MITRE ATT&CK tag

Add MITRE ATT&CK tactics and techniques that apply to this CVE.

Execution

TECHNIQUES	VALIDATION
Command and Scripting Interpreter	VALIDATED
Command and Scripting Interpreter: Unix Shell	VALIDATED

Metasploit Module

exploit/linux/http/webmin_backdoor

CISA KEV Listed · Common in enterprise · Easy to weaponize · Gives privileged access · Observed in ransomware attacks · Unauthenticated · Vulnerable in default configuration

Description

An issue was discovered in Webmin <=1.920. The parameter old in password_change.cgi contains a command injection vulnerability.

Ratings & Analysis | Vulnerability Details

Add Assessment

Log in to add an Assessment

15

wvu-r7 (435) 100 2

August 21, 2019 3:12am UTC (6 years ago) • Edited 2 years ago

Ratings

ATTACKER VALUE Very High

EXPLOITABILITY Very High

ATTACKER VALUE
VERY HIGH

42

Webmin password_change.cgi Command Injection

This was a supply chain attack: http://www.webmin.com/exploit.html. The backdoor was introduced in a version that was "exploitable" in the default install. Version 1.890 is the money. Anything after requires a non-default setting.

Note that SourceForge installs are affected, but GitHub checkouts aren't.

ETA: Metasploit added an exploit module.

This site uses cookies for anonymized analytics. For more information or to change your cookie settings, view our Cookie Policy.

busterb (317) 50

August 20, 2019 6:37pm UTC (6 years ago) • Edited 6 years ago

Ratings

ATTACKER VALUE Very High

EXPLOITABILITY

Technical Analysis

This is bound to have many vulnerabl e used by novice admins.

Quick Cookie Notification

This site uses cookies for anonymized analytics to improve the site.

Rapid7 will never sell the data collected on this site.

View our Cookie Policy for full details

Log in to Add Reply

ZM-20-20 (5)

January 30, 2021 1:40am UTC (5 years ago) • Edited 5 years ago

Ratings

ATTACKER VALUE Very High

EXPLOITABILITY High

Common in enterprise | Easy to weaponize | Gives privileged access

Technical Analysis

Almost 2 years later and this is still found in the wild.

Log in to Add Reply

bwatters-r7 (204) 40

August 22, 2019 10:22pm UTC (6 years ago) • Edited 6 years ago

Ratings

ATTACKER VALUE Very High

EXPLOITABILITY Very High

Technical Analysis

This is a terrible situation for any development team. A hacker took over a server that managed webmin code and changed the code in a subtle way to allow them (or others) to execute commands as root on computers running Webmin. It took nearly a year and a half for the attack to be discovered and fixed.

Log in to Add Reply

jrobles-r7 (40) 10

August 20, 2019 6:02pm UTC (6 years ago) • Edited 6 years ago

ATTACKER VALUE
VERY HIGH

42

Webmin password_change.cgi Command Injection

EXPLOITABILITY Very High

Technical Analysis

I tested Webmin v1.900 and the password change page was not available by default, however it is a reasonable option to have.

This site uses cookies for anonymized analytics. For more information or to change your cookie settings, view our Cookie Policy.

Log in to Add Reply

2

sgonzalez-r7 (8)

August 26, 2019 4:31pm UTC (6 years ago) • Edited 6 years ago

Ratings

ATTACKER VALUE

EXPLOITABILITY

Quick Cookie Notification

This site uses cookies for anonymized analytics to improve the site.

Rapid7 will never sell the data collected on this site.

View our Cookie Policy for full details

Log in to Add Reply

1

P1d0f (2)

July 10, 2020 4:11am UTC (6 years ago) • Edited 6 years ago

Ratings

ATTACKER VALUE Very High

EXPLOITABILITY High

Easy to weaponize Unauthenticated

Technical Analysis

High Vulnerability

Log in to Add Reply

1

69 (2)

February 28, 2020 4:26pm UTC (6 years ago) • Edited 6 years ago

Ratings

ATTACKER VALUE Very High

EXPLOITABILITY Very High

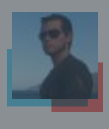
Easy to weaponize Gives privileged access

Technical Analysis

This vulnerability is very easy to exploit – without the need for any tools specialized for this attack.

Log in to Add Reply

0



KoelhoSec (1)

April 09, 2021 2:48am UTC (5 years ago) • Edited 5 years ago

Ratings

ATTACKER VALUE
VERY HIGH

42

Webmin password_change.cgi Command Injection

Unauthenticated Vulnerable in default configuration

Technical Analysis

MetaSploit module available:
exploit/linux/http/webmin_backdoor

This site uses cookies for anonymized analytics. For more information or to change your cookie settings, view our Cookie Policy.

Description:
This module exploits a backdoor in Webmin versions 1.890 through
1.920. Only the SourceForge downloads were backdoored, but they are

See More

Log in to Add Reply

Quick Cookie Notification

This site uses cookies for anonymized analytics to improve the site.

Rapid7 will never sell the data collected on this site.

View our Cookie Policy for full details

This site uses cookies for anonymized analytics. For more information or to change your cookie settings, view our Cookie Policy.