Privilege Escalation admin user to root user in hestiacp/hestiacp

2

Valid Reported on Jul 22nd 2022

Description

"admin" user has sudo rights and can gain root access. By default sudo installation "admin" group has root rights. "admin" user created by hestia installation and this user is also in "admin" group. if the attackers access "admin" user, can gain root access.

Proof of Concept

```
root@server:/home/t# sudo -u admin sudo -l
Matching Defaults entries for admin on server:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/

User admin may run the following commands on server:
    (ALL) ALL
    (root) NOPASSWD: /usr/local/vesta/bin/*
    (root) NOPASSWD: /usr/local/hestia/bin/*
```

admin user can run any commands as root with `(ALL) ALL` permission.

Fix

Change `%admin ALL=(ALL) ALL` to `# %admin ALL=(ALL) ALL` in "/etc/sudoers" file with visudo.

Impact

Attackers can gain root access with admin user.

References

- https://steflan-security.com/linux-privilege-escalation-sudo-commands-binaries/#:~:text=Sudo%20is%20a%20Linux%20utility,escalate%20their%20privileges%20to%20root.

CVE
CVE-2022-2626
(Published)

Vulnerability Type
CWE-266: Incorrect Privilege Assignment

Severity
Critical (9.1)

Registry
Other

Affected Version
1.6.4 (latest version)

Visibility
Public

Status
Fixed

Found by

imp
@redstarp2
legend

This report was seen 575 times.

We are processing your report and will contact the **hestiacp** team within 24 hours. 4 months ago

We have contacted a member of the **hestiacp** team and are waiting to hear back 4 months ago

Jaap Marcus 4 months ago Maintainer

We use by default

https://github.com/hestiacp/hestiacp/blob/main/install/deb/sudo/admin

On my test server:
Matching Defaults entries for admin on dev:

Matching Defaults entries for admin on dev:
env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin, env_keep=VESTA, env_keep+=HESTIA, !syslog, !requiretty

User admin may run the following commands on dev:
(root) NOPASSWD: /usr/local/vesta/bin/*
(root) NOPASSWD: /usr/local/hestia/bin/*

It looks like you are using a VM provider that creates the default admin user/group with sudo permissions.

imp 4 months ago Researcher

By default sudo installation on Ubuntu 18.04 and ubuntu 20.04 creates `/etc/sudoers` file.

Example `/etc/sudoers` file;
https://gist.github.com/alitoufighi/679304d9585304075ba1ad93f80cce0e

Contents of default `/etc/sudoers` file;

```
root@server:/etc# cat sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/
Defaults        use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
```

```
# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.

#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
```

Vulnerability does not exists in `https://github.com/hestiacp/hestiacp/blob/main/install/deb/sudo/admin` file. Hestia installation creates user named "admin" and add this user to "admin" group you can check it with id command ;

```
admin@server:~$ id
uid=1001(admin) gid=1001(admin) groups=1001(admin)
```

My test Env;


```
root@server:/etc# uname -a
```

```
Linux server.talhagunay.com 5.15.0-41-generic #44-Ubuntu SMP Wed Jun 22 14:20:53 UTC 2
```

```
root@server:/etc# cat /etc/issue
Ubuntu 22.04 LTS \n \l
```

Could you please check output of this command on ubuntu environment

```
sudo -u admin sudo -l
```

imp 4 months ago Researcher

Hi, is there any updates? and could you assign CVE for this vulnerability ?

We have sent a follow up to the **hestiacp** team. We will try again in 7 days. 4 months ago

Jaap Marcus modified the Severity from Critical (9.9) to Critical (9.1) 4 months ago

Jaap Marcus assigned a CVE to this report 4 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Jaap Marcus validated this vulnerability 4 months ago

imp has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Jaap Marcus marked this as fixed in **1.6.6** with commit **b178b9** 4 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation