Improper Authorization in phpipam/phpipam

0

Valid Reported on Feb 3rd 2022

Description

In phpIPAM 1.4.5, a normal user with the role of `User` could view/read the log files via show-logs.php, error_logs.php and access_logs.php endpoints. It is supposedly accessible by the `Administrator` only.

Proof of Concept

Tested version: phpIPAM 1.4.5

_
Affected endpoints:
1 GET/POST http://{HOST}/app/tools/logs/show-logs.php
2 POST http://{HOST}/app/dashboard/widgets/error_logs.php
3 POST http://{HOST}/app/dashboard/widgets/access_logs.php

_
Steps to reproduce:
1 Go to `http://{HOST}/app/tools/logs/show-logs.php`
2 Login as a user with the role of `User` .
3 We can read the log files detailing username, IP address, event, severity and date.

_
In normal user UI
PoC endpoint 1: GET
PoC endpoint 1: POST
PoC endpoint 2: POST
PoC endpoint 3: POST

Impact

This vulnerability is capable of revealing sensitive data exposure of relevant parties such as username, IP address, event, severity and date. Since the normal user can vie
usernames, he/she could conduct a dictionary/brute-force attack on the logi
authenticate with. He/she could also know the origin IP address of the admin to further the

attack.

Occurrences

access_logs.php L8-L15 | error_logs.php L8-L15 | show-logs.php L15-L21

CVE
CVE-2022-1224
(Published)

Vulnerability Type
CWE-285: Improper Authorization

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

Faisal Fs
@faisalfs10x
unranked

Fixed by

garyallan
@garyallan
maintainer

This report was seen 732 times.

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

Faisal Fs modified the report 10 months ago

Faisal Fs modified the report 10 months ago

Chat with us

Faisal Fs ⚔️ modified the report 10 months ago

We have contacted a member of the **phpipam** team and are waiting to hear back 10 months ago

We have sent a follow up to the **phpipam** team. We will try again in 7 days. 10 months ago

We have sent a second follow up to the **phpipam** team. We will try again in 10 days. 9 months ago

We have sent a third and final follow up to the **phpipam** team. This report is now considered stale. 9 months ago

A **phpipam/phpipam** maintainer has acknowledged this report 8 months ago

garyallan modified the report 8 months ago

garyallan validated this vulnerability 8 months ago

Faisal Fs ⚔️ has been awarded the disclosure bounty ✅

The fix bounty is now up for grabs

garyallan marked this as fixed in **1.4.6** with commit **f6a49f** 8 months ago

garyallan has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

error_logs.php#L8-L15 has been validated ✅

show-logs.php#L15-L21 has been validated ✅

access_logs.php#L8-L15 has been validated ✅

Sign in to join this conversation