Improper Access Control in phpipam/phpipam

Valid Reported on Feb 3rd 2022

Description

In phpIPAM 1.4.5, a normal user with the role of `User` could download or export IP subnets that may contain sensitive information related data such as IP address, IP state, MAC, owner, hostname and device via export-subnet.php endpoint. The bug is the export-subnet.php should verify the user has at least read permission to the subnet it is exporting and it does not.

Proof of Concept

Tested version: phpIPAM 1.4.5
Parameter: `subnetId`
Steps to reproduce:
1 Login as user with the role of User.
2 Go to `http://{HOST}/app/subnets/addresses/export-subnet.php?subnetId=1&ip_addr=on&state=on&description=on&hostname=on&firewallAddressObject=on&mac=on&owner=on&switch=on&port=on&note=on&location=on&filename=phpipam_subnet_export.xls`
3 We can export any related subnet data by changing subnetId parameter value with any running number such as 1, 2, 3 and so forth.

Impact

This vulnerability is capable of Improper Access Control and sensitive data exposure of related party.

CVE
CVE-2022-1223
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

Faisal Fs ⚔️
@faisalfs10x
unranked

Fixed by

garyallan
@garyallan
maintainer

This report was seen 917 times.

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

Faisal Fs ⚔️ modified the report 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 ✖

Sign in to join this conversation