SYNACKTIV
DIGITAL SECURITY

# 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<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps3 |

# Technical description and proof-of-concept

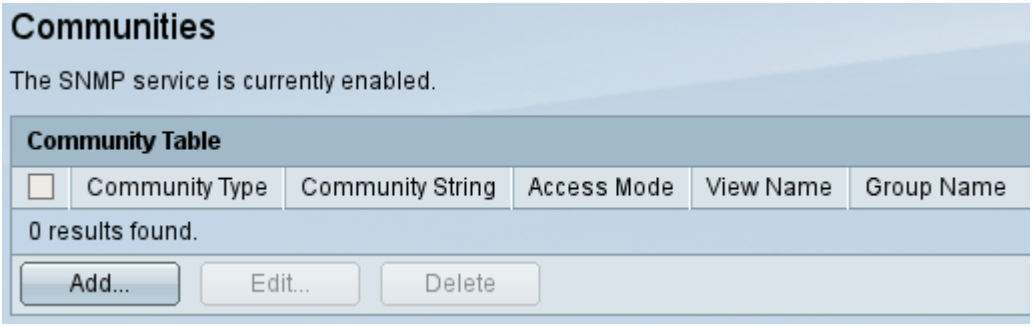
## Attack scenario

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.

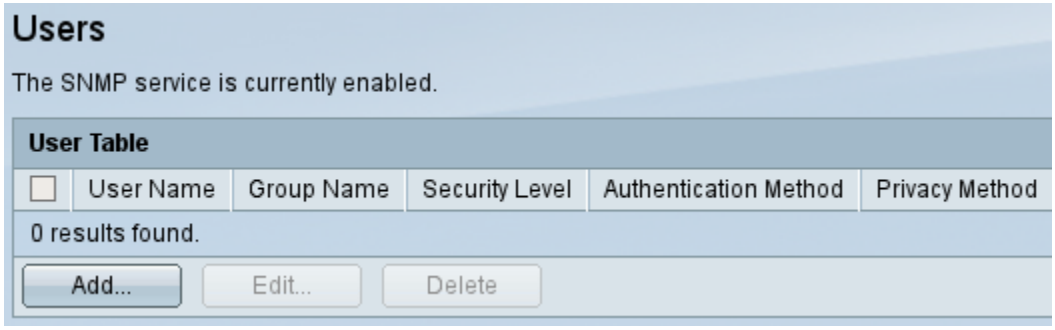
## Vulnerability discovery

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:



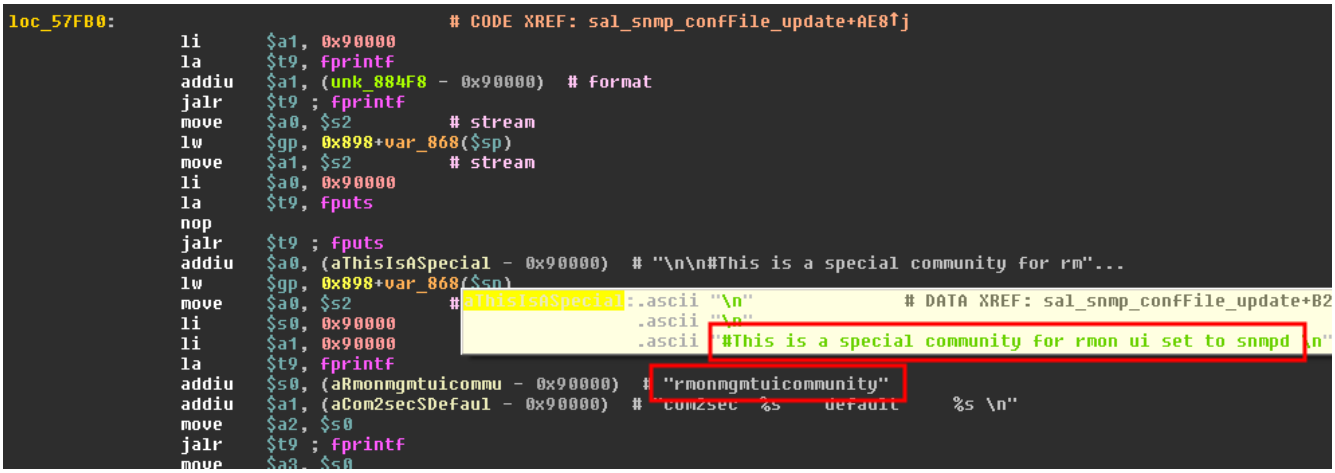

The SNMP part of the “show run” output only contains 1 line:

```
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.




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

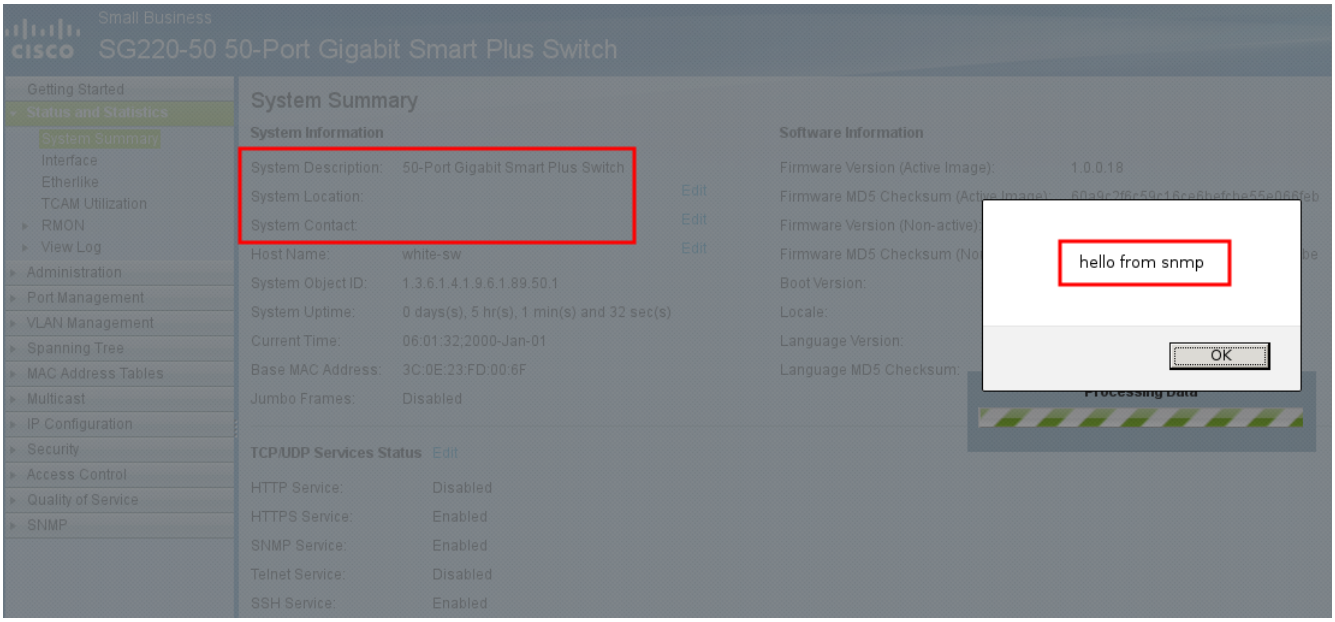
The following *snmpwalk* command will dump all the switch OID:

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

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

```
$ snmpset -v1 -c rmonmgmtuicommunity TARGET_IP sysLocation.0 s \
      '<script>alert(["hello","from","snmp"].join(String.fromCharCode(32)))</script>'

SNMPv2-MIB::sysLocation.0 = STRING:
<script>alert([\"hello\",\"from\",\"snmp\"].join(String.fromCharCode(32)))</script>
```




## Remediation

Disable the SNMP service.