SYNACKTIV
DIGITAL SECURITY

Web console denial of service in Cisco SG220 series

Security advisory

12/09/2015

Renaud Dubourguais
Nicolas Collignon

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 having a TCP access to the switch's web console to trigger a denial of service on the network service.

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 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps2

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 TCP access to the switch's web console (HTTP or HTTPS).

Vulnerability discovery

Using a web proxy such as BurpSuite to sniff, tamper and replay administration HTTP requests, Synacktiv discovered that sending a craft HTTP request to the switch leads to the web console crash.

Impact

A successful exploitation will make the web console unreachable. The service has to be manually restarted using another mean (SSH, Telnet or console).

Proof of concept

The following cURL command will crash the switch's web console (no authentication is required):

```
$ curl -i -s -k  -X 'POST' 'https://switch/cgi/set.cgi?cmd=aaa_userAdd'
```

Technically, the switch expects a request body in the POST request. As we don't provide a body, the request parser will crash.