At a glance:

IR Number	FG-IR-16-023
Date	Aug 17, 2016
Risk	●●●●○
Impact	Remote administrative access
CVE ID	CVE-2016-6909 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6909)

PSIRT Advisory

Cookie Parser Buffer Overflow Vulnerability

Summary

FortiGate firmware (FortiOS) released before Aug 2012 has a cookie parser buffer overflow vulnerability. This vulnerability, when exploited by a crafted HTTP request, can result in execution control being taken over.
Affected firmware versions are lower versions of 4.x firmware release.
FortiOS 5.x firmware is NOT affected.
Affected FortiSwitch firmware versions are 3.4.2 and below.

Impact

Remote administrative access

Affected Products

FortiGate (FortiOS):
4.3.8 and below
4.2.12 and below
4.1.10 and below

FortiSwitch:
3.4.2 and below

Solutions

Upgrade to release 5.x.

Upgrade to release 4.3.9 or above for models not compatible with FortiOS 5.x.

Note that the following AV and IPS signatures block the potential attacks:

- ELF/Adows.A!exploit since AV DB 36.803
- IPS signature: FortiGate.Cookie.Buffer.Overflow since IPS DB 8.935

FortiSwitch:

- Upgrade to release 3.4.3

Workarounds:
FortiOS:

- Disable admin access via HTTP and HTTPS on all interfaces, and use SSH instead
- On 4.3, if HTTP or HTTPS access is mandatory, one can restrict access to HTTP and HTTPS to a minimal set of authorized IP addresses, via the Local In policies
- On 4.2 and 4.1, if HTTP or HTTPS access is mandatory, one can restrict access to the administration interfaces (including HTTP and HTTPS access) to a minimal set of authorized IP addresses, via the trusthost commands

FortiSwitch:

- Disable admin access via HTTP and HTTPS on all interfaces, and use the CLI instead. Alternatively, restrict access to the administration interfaces (including HTTP and HTTPS access) to a minimal set of authorized IP addresses, via the trusthost commands

Acknowledgement

The vulnerability was initially reported to Fortinet in August 2012 by Florian Gaultier of SCRT. Back then, it was mentioned in FortiOS 4.3.9 release notes.