CERT-EU Security Advisory 2016-135
Leak of hacking tools targeting Fortinet devices

30/08/2016

Summary
On 13th of August, a previously unknown group called "Shadow Brokers" publicly released a large number of hacking tools they claimed were used by the "Equation Group". They also offered to sell to the highest bidder an additional set of tools. The leaked files included discovery tools, exploitation tools, implants and documentation on how to use them. The files in the leak have date stamps not later than October 2013. The targeted devices include:

- Fortigate firewalls, for versions of firmware superseded in 2012.

Fortinet has issued advisory and patches/workarounds for the exposed vulnerability:
http://fortiguard.com/advisory/FG-IR-16-023

Impact
The leaked tools are fully functional and would indeed compromise the targeted devices. Initial exploitation would not be noticed by administrators as the tools used unknown vulnerabilities. Also, it would not necessarily be avoidable by well-configured devices either. In compromising these devices, the adversary would gain rogue external access to an infrastructure protected by a firewall.

Specific risk assessment and recommendations
EGREGIOUSBLUNDER (HTTP/HTTPS remote code execution CVE-2016-6909)

- FortiGate (FortiOS) – 4.3.8 and below, 4.2.12 and below, 4.1.10 and below
- FortiSwitch – 3.4.2 and below

FortiGate (FortiOS) releases 5.x are **not** impacted by this vulnerability

Risk Assessment of CVE-2016-6909 on FortiGate and FortiSwitch range of products

Criticality of the assets	Critical	Normal
Admin access via HTTP or HTTPS enabled on external (Untrusted) interface	**HIGH**	**HIGH**
Admin access via HTTP or HTTPS enabled on internal (Trusted) interface	**MEDIUM**	**LOW**

Recommendations for HIGH risk response

1. Collect forensic evidence:

- Execute and store the output of **`show`** commands `like get system status`, `get hardware status`, `show full-configuration`;
- Recover logs and store them securely.

2. Upgrade Software to the latest version.

3. Harden Configuration:

FortiOS:

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

Change admin credentials.

4. Update FortiGuard IPS/IDS signatures and deploy the following SNORT rule to capable sensors:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"FortiGate.Cookie.Buffer.Overflow";
flow:to_server,established;  content:"APSCOOKIE";  fast_pattern:only;  content:"APSCOOKIE";
http_cookie; content:"Payload"; nocase; http_cookie; content:"AuthHash"; nocase; http_cookie;
content:!"%0A";  nocase;  http_cookie;  within:50;  content:!"|0A|";  nocase;  http_cookie;
within:55; metadata:service http; classtype:attempted-admin; sid:9999999; rev:1; )
```

5. Stay alerted for the future software releases.

Recommendation for LOW and MEDIUM risk response

1. Upgrade Software to the latest version.

2. Harden Configuration.

3. Update FortiGuard IPS/IDS signatures.

4. Stay alerted for the future software releases.