computer emergency response team CERT-EU for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2016-0138

IKEv1 vulnerability targeting CISCO devices

21/09/2016

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.

CISCO has issued advisories and patches/workarounds for the exposed vulnerabilities impacting CISCO ASA and PIX firewalls

On 16th of September, after a code review on other products, CISCO published a new advisory related to IKEv1 implementation in Cisco IOS, Cisco IOS XE, and Cisco IOS XR Software:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1

Impact

An attacker could exploit this vulnerability by sending a crafted IKEv1 packet to a vulnerable device configured to accept IKEv1 security negotiation requests. It could allow the attacker to retrieve memory contents, which could lead to the disclosure of confidential information.
IKEv1 is used by several features on CISCO devices like:

- LAN-to-LAN VPN
- Remote access VPN (excluding SSLVPN)
- Dynamic Multipoint VPN (DMVPN)
- Group Domain of Interpretation (GDOI)

Affected Products (CVE-6415)

Cisco IOS XR Software

- Cisco IOS XR 4.3.x, 5.0.x, 5.1.x and 5.2.x

Cisco IOS XE Software

- All versions

Cisco IOS Software

- See https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1

As of today, there is no patch or workaround available.

Recommendations

1. Determine if IKE Ports are Open on running devices and configured features using IKEv1:

- Run the `show udp` command and look for UDP ports 500,4500, 848 or 4848 open
- Run the `show run | include crypto map|tunnel protection ipsec|crypto gdoi` command and look if the output of this command contains either `crypto map, tunnel protection ipsec, or crypto gdoi`

2. Disable IKEv1 functionalities if possible until the fix for CVE-2016-6415 is released.

3. Deploy Snort rules 40220, 40221, and 40222 and/or CISCO 7699-0 to detect exploitation attempts

Appendix: SNORT Rules

```
alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"SERVER-OTHER Cisco IOS
Group-Prime memory disclosure attempt"; flow:to_client; dsize:>2000;
content:"|0B 10 05 00|"; depth:8; offset:16; byte_test:4,>,2000,4,relative;
metadata:policy balanced-ips drop, policy security-ips drop;
classtype:attempted-recon; sid:40220; rev:2;)
```

```
alert udp $EXTERNAL_NET any -> $HOME_NET 500 (msg:"SERVER-OTHER Cisco IOS
Group-Prime MD5 memory disclosure attempt"; flow:to_server; dsize:>2000;
content:"|00 00 00 00 00 00 00 00|"; depth:8; offset:8; content:"|00 00 00
01 00 00 00 01|"; depth:8; offset:32; content:"|01 01 04 01|"; within:4;
distance:4; content:"|80 02 00 01 80 04 00 01 00 06|"; distance:0;
fast_pattern; byte_test:2,>,2000,0,relative; metadata:policy balanced-ips
drop, policy security-ips drop; classtype:attempted-recon; sid:40221;
rev:2;)
```

```
alert udp $EXTERNAL_NET any -> $HOME_NET 500 (msg:"SERVER-OTHER Cisco IOS
Group-Prime SHA memory disclosure attempt"; flow:to_server; dsize:>2000;
content:"|00 00 00 00 00 00 00 00|"; depth:8; offset:8; content:"|00 00 00
01 00 00 00 01|"; depth:8; offset:32; content:"|01 01 04 01|"; within:4;
distance:4; content:"|80 02 00 02 80 04 00 01 00 06|"; distance:0;
fast_pattern; byte_test:2,>,2000,0,relative; metadata:policy balanced-ips
drop, policy security-ips drop; classtype:attempted-recon; sid:40222;
rev:2;)
```