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

CERT-EU Security Advisory 2016-0133

Leak of hacking tools targeting CISCO firewalls

22/08/2016

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:

- CISCO Adaptive Security Appliance (ASA) firewalls, current products ;
- CISCO PIX firewalls, an end of line product, not supported any more since 2009.

CISCO has issued advisories and patches/workarounds for the exposed vulnerabilities:
http://blogs.cisco.com/security/shadow-brokers
http://tools.cisco.com/security/center/viewErp.x?alertId=ERP-56516

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. And 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 or a virtual private network.

Specific risk assessment and recommendations

EXTRABACON (SNMP remote code execution CVE-2016-6366)

- PIX – VULNERABLE no fix available
- ASA – Newly found defect (CSCva92151). Fixed image will be available for download this week
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

EPICBANANA (CLI remote code execution)

- PIX – VULNERABLE no fix available
- ASA – Known defect (CSCtu74257). Fixed in version 8.4(3).
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli

BENIGNCERTAIN (IKE vulnerability)

- PIX – VULNERABLE pre 7.0. Fixed from version 7.0 onwards
- ASA – NOT VULNERABLE

Other vulnerabilities not necessarily related to this leak require risk mitigation. As an example, early 2016 CISCO released an advisory related to an Internet Key Exchange Buffer Overflow Vulnerability (CVE-2016-1287):
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike

Risk Assessment of (CVE-2016-6366) and (CVE-2016-1287) on CISCO ASA range of products

Criticality of the assets	Critical	Normal
SNMP enabled on external (Untrusted) interface	HIGH	HIGH
SNMP enabled on internal (Trusted) interface	HIGH	MEDIUM
VPN Enabled	HIGH	HIGH
SNMP and VPN not enabled	LOW	LOW

Recommendations for HIGH risk response

1. Collect forensic evidence

- Execute and store the output of show commands like show region, show version, show running-configuration all, show tech-support;
- Create a memory dump, compute hash and store in a secure manner.

2. Perform an ASA Software Integrity Check

Follow vendor's documentation on integrity checks:
http://www.cisco.com/c/en/us/about/security-center/intelligence/asa-integrity-assurance.html
If the Software Integrity Check fails then a complete incident response procedure must follow along with an impact assessment.

3. Upgrade Software to the latest version

4. Harden Configuration

Disable SNMP if possible until the fix for CVE-2016-6366 is released. Follow vendor's guide on hardening:
http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Besides hardening and before restoring operations ensure that all pre-shared keys and certificates that are used for the IKE negotiations are changed along with the passwords for accessing the appliance. Reassess the algorithms used for encryption and consider using the latest elliptic curves.

http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_16-002_Weaknesses%20in%20Diffie-Hellman%20Key%20v1_0.pdf

5. Deploy Snort rules 3:39885, 1:36903 and 1:37674 and/or CISCO 7655-0, 7169-0 and 7169-1.

Although it seems more efficient when deployed on the ISP's side they may be triggered when there is already an infected computer inside the perimeter.

6. Stay alerted for the future software releases.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

Recommendation for MEDIUM risk response

1. Upgrade Software to the latest version

2. Harden Configuration

Disable SNMP if possible until the fix for CVE-2016-6366 is released.

Besides hardening and before restoring operations ensure that all pre-shared keys and certificates that are used for the IKE negotiations are changed along with the passwords for accessing the appliance. Reassess the algorithms used for encryption and consider using the latest elliptic curves.

http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_16-002_Weaknesses%20in%20Diffie-Hellman%20Key%20v1_0.pdf

3. Deploy Snort rules 3:39885, 1:36903 and 1:37674 and/or CISCO 7655-0, 7169-0 and 7169-1.

4. Stay alerted for the future software releases.

Recommendation for LOW risk response

1. Upgrade Software to the latest version

2. Review Configuration and deploy best practices.

Reassess the algorithms used for encryption and consider using the latest elliptic curves.

http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_16-002_Weaknesses%20in%20Diffie-Hellman%20Key%20v1_0.pdf

3. Deploy Snort rules 3:39885, 1:36903 and 1:37674 and/or CISCO 7655-0, 7169-0 and 7169-1.

4. Stay alerted for the future software releases.