INCIDENT RESPONSE, FORENSICS, AND VULNERABILITY MANAGEMENT
LESSONS LEARNED USING MODERN TECHNIQUES

Omar Santos
Principal Engineer, Cisco PSIRT
os@cisco.com | Twitter: @santosomar
A FEW YEARS AGO…

YOU WAKE UP IN THE MORNING AND THERE IS A NEW BRANDED VULNERABILITY…
NOWADAYS... YOU WAKE UP IN THE MORNING AND THERE IS A NEW LEAK, BREACH, BRANDED CRITICAL VULNERABILITY...
CASE STUDY 1
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.
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:

<table>
<thead>
<tr>
<th>Directory Name</th>
<th>Exploit Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>EGBL</td>
<td>E GreggiousBlunder</td>
</tr>
<tr>
<td>ELBA</td>
<td>EligibleBachelor</td>
</tr>
<tr>
<td>ELBO</td>
<td>EligibleBombshell</td>
</tr>
</tbody>
</table>
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
Security

The Shadow Brokers EPICBANANA and EXTRABACon Exploits

Omar Santos - August 17, 2016 - 0 Comments

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 disclosures, Cisco started investigating internal products to determine whether any Cisco internal systems were affected by the attack. We have not found any evidence of this being the case.
Cisco Adaptive Security Appliance SNMP Remote Code Execution Vulnerability

Summary

A vulnerability in the Simple Network Management Protocol (SNMP) code of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a reload of the affected system or to remotely execute code.

The vulnerability is due to a buffer overflow in the affected code area. The vulnerability affects all versions of SNMP (versions 1, 2c, and 3) when enabled on a virtual or physical Cisco ASA device. An attacker could exploit this vulnerability by sending crafted SNMP packets to an SNMP-enabled interface on the affected system. An 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. The attacker must know the SNMP community string to exploit this vulnerability.

Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability cannot be exploited from external networks.
Cisco Event Response: Cisco ASA and IOS Vulnerabilities

Doc ID: ERP-56516
First Published: 2016 August 17 18:50 GMT
Last Updated: 2016 September 21 18:39 GMT
Version: 1.1

Summary

- On August 15, 2016, Cisco was alerted to information posted online by the alleged Shadow Brokers group, which claimed to possess disclosures from the Equation Group. The posted materials included exploits for firewall products from multiple vendors. The Cisco products mentioned were the PIX and ASA firewalls.
- On September 16, 2016 Cisco identified an IKEv1 Information Disclosure Vulnerability in Cisco IOS that is related to variations of the exploits published.
- The Cisco PSIRT has investigated the published information and determined it provides exploits of two Cisco product vulnerabilities in ASA and one vulnerability in Cisco IOS.

Details

In accordance with the Cisco security vulnerability disclosure policy, Cisco Security Advisories have been published:

(17 August 2016) Cisco Adaptive Security Appliance CLI Remote Code Execution Vulnerability: This vulnerability is a known defect that was addressed in a Release Note Enclosure in 2011.
HOW DO YOU INVESTIGATE, FIX, DISCLOSE, AND HELP YOUR CUSTOMERS IN MINUTES OR HOURS?
PROCESS - WHAT PROCESS?

- POST DISCLOSURE ACTIVITIES
- PATCHES / FIXES
- INTERNAL COMMUNICATIONS
  "HOT PAGES", DASHBOARDS, TAC, SERVICES, SALES, ENGINEERING, EXECS
- TECHNICAL COMPETENCY
  APPROPRIATE ENGINEERING RESOURCES, AUTOMATION
- EXTERNAL COMMUNICATIONS
  CUSTOMERS, PARTNERS, PR/MEDIA, OTHERS
- OWNERSHIP
  LEADERSHIP AND OWNERSHIP OF ISSUE
- LESSONS LEARNED
- MITIGATIONS
CASE STUDY 2
Cisco WebEx Browser Extension Remote Code Execution Vulnerability

Summary
A vulnerability in Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows.

The vulnerability is due to a design defect in an application programming interface (API) response parser within the plugin. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.
Cisco drops patch for nasty WebEx remote code execution hole

Patch, then patch this, this, this, this, this, this, this, and this

By Darren Pauli 16 Sep 2016 at 01:54

Cisco is warning admins to apply a patch for a critical WebEx vulnerability, one of nine fixed this week.

The remote code execution flaw (CVE-2016-1482) could allow attackers to execute arbitrary commands on WebEx servers.

Admins can only apply the patch and do not have an option to deploy work-around mitigations.

"A vulnerability in Cisco WebEx Meetings Server could allow an unauthenticated, remote attacker to bypass security restrictions on a host located in a DMZ and inject arbitrary commands on a targeted system," Cisco wrote in an advisory.

"The vulnerability is due to insufficient sanitization of user-supplied data processed by the affected software. An attacker could exploit this vulnerability by injecting arbitrary commands into existing application scripts running on a targeted device located in a DMZ [and] could allow an attacker to execute arbitrary commands on the device with elevated privileges."
Critical

Summary

A vulnerability in the role-based access control (RBAC) functionality of Cisco Prime Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to access sensitive information or execute arbitrary code with root privileges on an affected system.

The vulnerability is due to the lack of authentication and authorization mechanisms for a debugging tool that was inadvertently enabled in the affected software. An attacker could exploit this vulnerability by remotely connecting to the debugging tool via TCP. A successful exploit could allow the attacker to access sensitive information about the affected software or execute arbitrary code with root privileges on the affected system.

Cisco has released software updates that address this vulnerability. There are no workarounds that...
A vulnerability in the role-based access control (RBAC) functionality of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to access sensitive information or execute arbitrary code with 'em-root' privileges on an affected system or 'admin' privileges on the vulnerable role. The vulnerability is due to the lack of authentication and authorization mechanisms for debugging tools that was inadvertently enabled in the affected software. An attacker could exploit this vulnerability by sending a crafted request through an affected Cisco DCNM appliance.
<table>
<thead>
<tr>
<th></th>
<th>Budget Constraints 39%</th>
<th>Lack of Knowledge 23%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compatibility Issues</td>
<td>32%</td>
<td>23%</td>
</tr>
<tr>
<td>Certification Requirements 25%</td>
<td></td>
<td>22%</td>
</tr>
<tr>
<td>Competing Priorities</td>
<td>24%</td>
<td>22%</td>
</tr>
<tr>
<td>Current Workload Too Heavy 24%</td>
<td></td>
<td>20%</td>
</tr>
</tbody>
</table>
OASIS CSAF: chartered to make a major revision to the Common Vulnerability Reporting Framework (CVRF) under a new name for the framework that reflects the primary purpose: a Common Security Advisory Framework (CSAF).

TC deliverables are designed to standardize existing practice in structured machine-readable vulnerability-related advisories and further refine those standards over time.
Invitation to comment on CSAF Common Vulnerability Reporting Framework (CVRF) v1.2 - ends July 20th

The official OASIS announcement can be found at the following link:
Invitation to comment on #CSAF Common Vulnerability Reporting Framework (#CVRF) v1.2 - ends July 20th
Submitted by censign on Tue, 2017-06-20 13:46

We are pleased to announce that CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2, the first release from the OASIS Common Security Advisory Framework (CSAF) TC, is now available for public review and comment.

CVRF is a language to exchange Security Advisories and provide for greater interoperability among products by ensuring that machine-readable security advisories can be produced and consumed much more broadly. The specification builds on the Common Vulnerability Reporting Framework (CVRF) 1.1 which was initiated by ICASI, the Industry Consortium for Advancement of Security on the Internet and contributed to OASIS.

For more information on CVRF and the CSAF TC, see the press release at https://www.oasis-open.org/news/pr/oasis-advances-standard-for-automated...

The documents and related files are available at:

CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2 Committee Specification Draft 01 / Public Review Draft 01
31 May 2017

PDF (Authoritative):
http://docs.oasis-open.org/csa/csvrf/cvrf/v1.2/csprd01/csa-cvrf-v1.2-cs...

HTML:
http://docs.oasis-open.org/csa/csvrf/cvrf/v1.2/csprd01/csa-cvrf-v1.2-cs...

Editable source:
http://docs.oasis-open.org/csa/csvrf/cvrf/v1.2/csprd01/csa-cvrf-v1.2-cs...

XML schemas:
http://docs.oasis-open.org/csa/csvrf/cvrf/v1.2/csprd01/schemas/

For your convenience, OASIS provides a complete package of the prose document and its associated files.
WE NEED TO MAINTAIN COMPETITIVE ADVANTAGE AND MOVE FAST!
CASE STUDY 3
HOW WE CREATED CODE YESTERDAY

closed
<source>
import ntplib
from OpenSSL import SSL
from django.http import HttpResponse
import datetime
import some_other_open_source_lib_omar_created
import super_vuln_library

def some_vuln_function(type, bits):
    pkey = crypto.PKey()
    pkey.generate_key(type, bits)
    return pkey
Open Source Used In Firepower System Version 6.2

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: 79E1171296-120762162
7.136 spring-aspects 4.1.9.RELEASE
    7.136.1 Available under license
7.137 spring-beans 4.1.9.RELEASE
    7.137.1 Available under license
7.138 spring-context 4.1.9.RELEASE
    7.138.1 Available under license
7.139 spring-core 4.1.9.RELEASE
    7.139.1 Available under license
7.140 spring-data-commons 1.11.2.RELEASE
    7.140.1 Available under license
7.141 spring-data-neo4j 3.4.2.RELEASE
    7.141.1 Available under license
7.142 spring-expression 4.1.9.RELEASE
    7.142.1 Available under license
7.143 spring-security-config 4.0.2.RELEASE
    7.143.1 Available under license
7.144 spring-security-core 4.0.2.RELEASE
    7.144.1 Available under license
7.145 spring-security-web 4.0.2.RELEASE
    7.145.1 Available under license
7.146 spring-tx 4.1.9.RELEASE
    7.146.1 Available under license
7.147 spring-web 4.1.6
    7.147.1 Available under license
7.148 spymemcached 2.8.4 :2.8.4
    7.148.1 Available under license
7.149 SQLite JDBC 3.7.2
Wait a minute.
MODERNIZE | ACCELERATE
PSIRT

Overview
Communities
Cisco Security Portal
Access our GitHub Repository

Cisco PSIRT openVuln API
- Automate Security Vulnerability Assessment
- Customize Cisco Vulnerability Notifications
- Use Open Security Standards

1 Overview
Find out how Cisco PSIRT openVuln API help.

2 Getting Started
Watch videos and technical documentation to get started with the Cisco PSIRT openVuln API.

3 Try the API Now!
Access the Cisco openVuln API to obtain Cisco Security Vulnerability information here.
Cisco PSIRT openVuln API Overview

The Cisco PSIRT openVuln API is a RESTful API that allows customers to obtain Cisco security vulnerability information in different machine-consumable formats. It supports industrywide security standards such as the
The Cisco PSIRT openVuln API is a RESTful API that allows customers to obtain Cisco Security Vulnerability information in different machine-readable formats. APIs are important for customers because they allow their technical staff and programmers to build tools that help them do their job more effectively (in this case, to keep up with security vulnerability information).

For more information about the Cisco PSIRT openVuln API visit https://developer.cisco.com/site/PSIRT/discover/overview.

For detailed steps on how to use the API go to: https://developer.cisco.com/site/PSIRT/get-started/getting-started.gsp.

This is a beta release of a swagger YAML for the Cisco PSIRT openVuln API.

To access the API sign in with your Cisco CCO account at https://apiconsole.cisco.com and register an application to receive a client_id and a client_secret.

You can then get your token using curl or any other method you prefer.

```
curl -s -k -H "Content-Type: application/x-www-form-urlencoded" -X POST -d "client_id=your_client_id" -d "client_secret=your_client_credentials" https://cloudsso.cisco.com/as/token.oauth2
```

You will receive an access token as demonstrated in the following example:

```
{"access_token": "I7om8AbDAieSiUX3sh0Njfu4J6", "token_type": "Bearer", "expires_in": 3599}
```

In Swagger, click on Change Authentication and enter the text "I7om8AbDAieSiUX3sh0Njfu4J6" (which is the token you receive).
Cisco Investigates and Average of 150 Open Source Vulnerability Reports Per Week
### Cisco Security Advisories and Alerts

#### Advisory/Alert

<table>
<thead>
<tr>
<th>Advisory/Alert</th>
<th>Impact</th>
<th>CVE</th>
<th>Last Updated</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>GNU glibc LD_LIBRARY_PATH Memory Corruption Vulnerability</td>
<td>High</td>
<td>CVE-2017-100366</td>
<td>2017 Jun 21</td>
<td>2.0</td>
</tr>
<tr>
<td>Linux Kernel Stack Guard Bypass Memory Corruption Vulnerability</td>
<td>High</td>
<td>CVE-2017-100364</td>
<td>2017 Jun 21</td>
<td>3.0</td>
</tr>
<tr>
<td>Network Security Services Empty SSLv2 Message Denial of Service Vulnerability</td>
<td>High</td>
<td>CVE-2017-7502</td>
<td>2017 Jun 21</td>
<td>2.0</td>
</tr>
<tr>
<td>Xen P2M Mapping Local Privilege Escalation Vulnerability</td>
<td>High</td>
<td></td>
<td>2017 Jun 21</td>
<td>1.0</td>
</tr>
<tr>
<td>Xen Grant Table Mapping Local Privilege Escalation Vulnerability</td>
<td>High</td>
<td></td>
<td>2017 Jun 21</td>
<td>1.0</td>
</tr>
<tr>
<td>Microsoft Windows Graphics Component Privilege Escalation Vulnerability</td>
<td>High</td>
<td>CVE-2017-8576</td>
<td>2017 Jun 21</td>
<td>1.0</td>
</tr>
<tr>
<td>Microsoft Windows DirectX Handling Privilege Escalation Vulnerability</td>
<td>High</td>
<td>CVE-2017-8579</td>
<td>2017 Jun 21</td>
<td>1.0</td>
</tr>
</tbody>
</table>
An update for Thunderbird is now available for Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Score (CVSS) is not available at this time.

Mozilla Thunderbird is a stand-alone email client.