Predictive CVE Hunting

BalCCon
September 9th, 2016

Director of Research Innovation
Research Team

ThreatConnect, Inc.

Cezanne Vahid
Research Intern
Research Team

ThreatConnect, Inc.

@ThreatConnect

@MalwareUtkonos

Working In A Small Team

Small Teams Need Big Tactics

Small Teams

- Must compete at the level of large teams
- Fight smarter
- Find new malware as fast as possible

Hypothesis

Malicious binaries exploiting new CVEs can be detected shortly after the zero day by hunting for CVE numbers in VirusTotal’s dataset using YARA rules. This process leverages the wide visibility provided by the collected group of antivirus companies on VirusTotal.

Definitions

cve.mitre.org

US-CERT
UNITED STATES COMPUTER
EMERGENCY READINESS TEAM

- CVE - Common Vulnerabilities and Exposures
- US-CERT - United States Computer Emergency Readiness Team
  - Part of Department of Homeland Security (DHS)
- NVD - National Vulnerability Database
  - Maintained by National Institute of Standards and Technology (NIST)

U.S. DEPARTMENT OF HOMELAND SECURITY

National
Vulnerability
Database
nvd.nist.gov

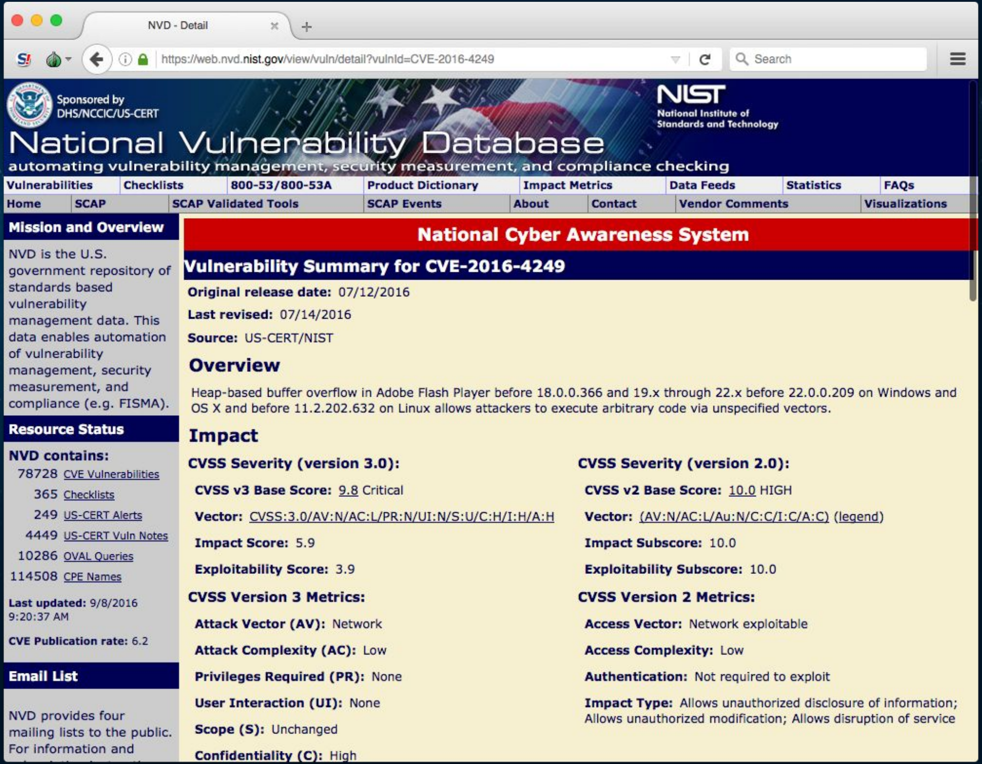
NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

YARA

YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic.

Example - CVE-2016-4249 (Adobe Flash)

Heap-based buffer overflow in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors.



National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

78728 CVE Vulnerabilities
365 Checklists
249 US-CERT Alerts
4449 US-CERT Vuln Notes
10286 OVAL Queries
114508 CPE Names

Last updated: 9/8/2016 9:20:37 AM

CVE Publication rate: 6.2

Email List

NVD provides four mailing lists to the public. For information and

National Cyber Awareness System

Vulnerability Summary for CVE-2016-4249

Original release date: 07/12/2016
Last revised: 07/14/2016
Source: US-CERT/NIST

Overview

Heap-based buffer overflow in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors.

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 9.8 Critical
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High

CVSS Severity (version 2.0):

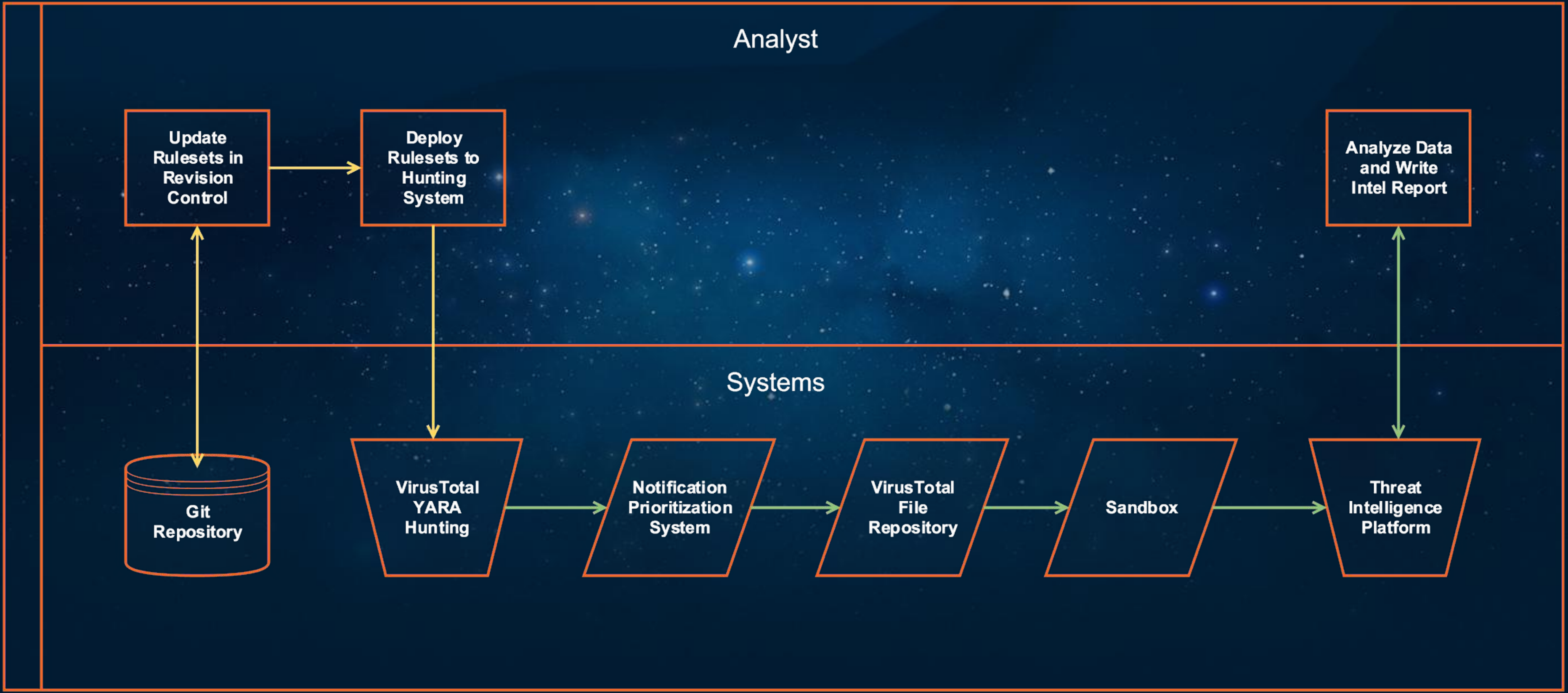
CVSS v2 Base Score: 10.0 HIGH
Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

YARA Hunting Process

Where It All Began


Analyst
Update Rulesets in Revision Control
Deploy Rulesets to Hunting System
Analyze Data and Write Intel Report
Systems
Git Repository
VirusTotal YARA Hunting
Notification Prioritization System
VirusTotal File Repository
Sandbox
Threat Intelligence Platform

Efficiencies

15% ave. reduction time to process & analyze a sample of interest.

Over **1500** samples this is **300** hours. Almost a week's worth of time in manually MOVING data.

30% increase in content production.

An analyst can now reclaim that **300** hours in additional analysis & production.

Predictive CVE Hunting

Fighting Above Our Weight Class

The YARA Rule Template

```
rule <name>
{
strings:

   $cve = /[Cc][Vv][Ee][_-]? ?\d{4}[_-]? ?\d{4}/

condition:

   ($cve or tags contains "<CVE Number>" or signatures
contains "<CVE Number>") and new_file and not tags
contains "zero-filled"
}
```

What is Important?

- Browser Vulerabilities
- Operating System Vulerabilities
  - Privilege escalation
  - Arbitrary code execution (especially remote)
- Java
- Flash
- PDF
- Silverlight
- Office Documents
- Mobile
  - iOS
  - Android

Hunting in Action

Has It Worked?

Near Miss - CVE-2015-0336

- Arbitrary code execution in Adobe Flash
- Nuclear EK - 3/19/2015
- Why did we miss it?
  - Rules only looking for CVE numbers in AV scanner results
- What happened?
  - A researcher, Kaffeine, found the first samples, uploaded them, and tagged them as CVE-2015-0336 thus bypassing our rules
- Added tags contains "<CVE Number>" to the template

Near Miss - CVE-2016-1019

- Arbitrary code execution in Adobe Flash
- Used to spread Cerber Ransomware 4/2/2016
- Why did we miss it?
  - New intern was only just getting trained
- What corrections were made?
  - We went backwards in time and deployed all the missing YARA signatures

All The Hits

- CVE-2015-1641
  - Allow remote attackers to execute arbitrary code via a crafted RTF document, aka "Microsoft Office Memory Corruption Vulnerability."
- CVE-2015-5122
  - Use-after-free vulnerability in the DisplayObject class in the ActionScript 3 (AS3) implementation in Adobe Flash Player
- CVE-2015-5119
  - Use-after-free vulnerability in the ByteArray class in the ActionScript 3 (AS3) implementation in Adobe Flash Player

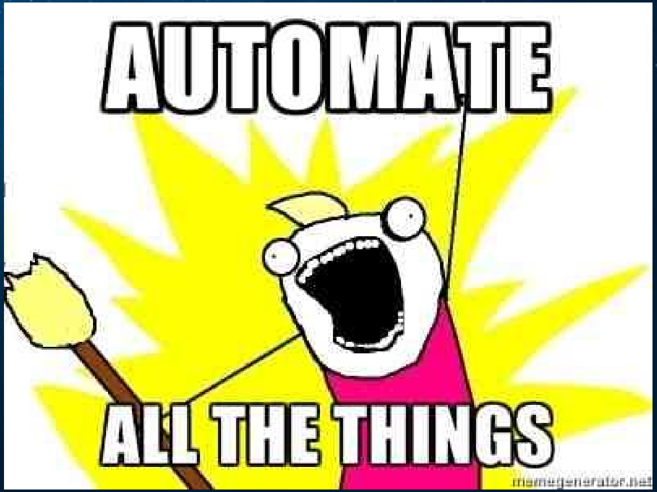
False-ish Positives

- Exploits may exist that are not weaponized, but exist in exploit databases
- Non-executables (text files and other documents)

Automate All The Things

Process Automation

- Intern writes software to replace himself
- Python and Selenium



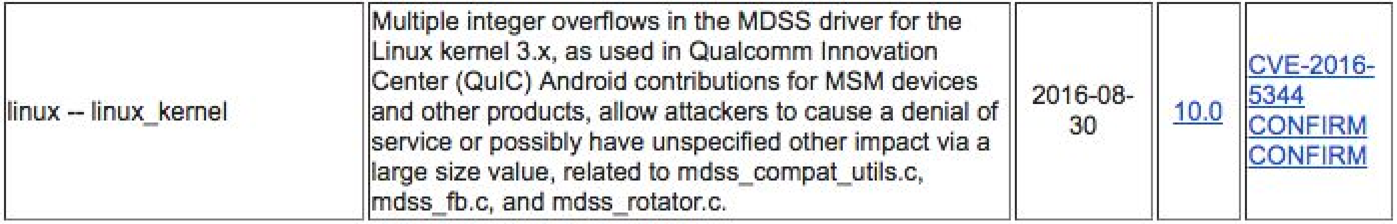
THREATCONNECT™

Part 1: Rule generation Python Script

1. Pull CVE information from US-CERT and NVD RSS feeds
2. Grab CVE Identifiers and titles from XML
3. Insert ID and title into Yara Rule Format
4. Upload to VT
5. Rinse & Repeat!

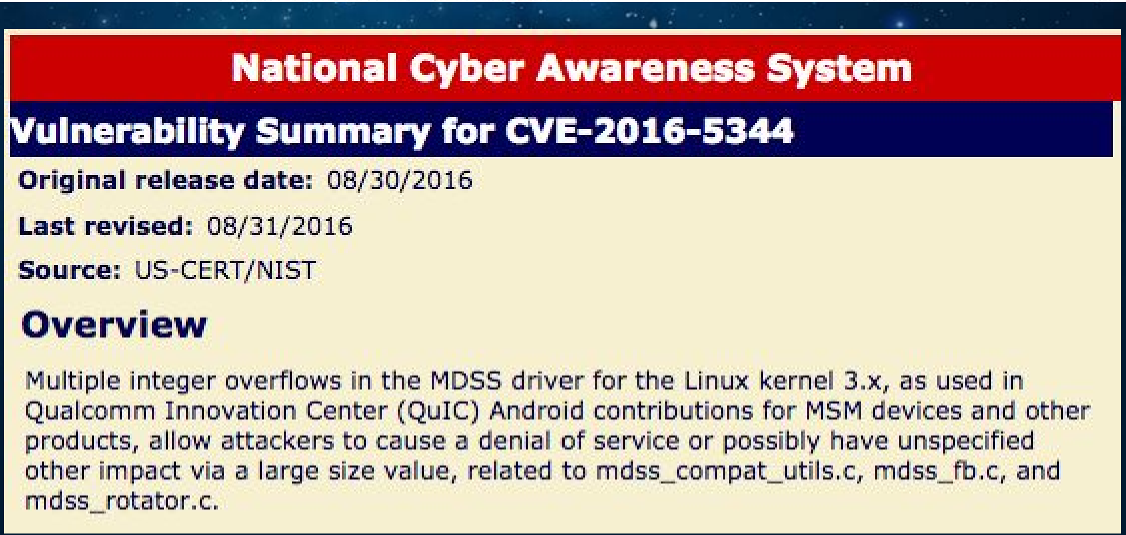
Collecting CVEs - Under Development

US-CERT Bulletin



linux -- linux_kernel	Multiple integer overflows in the MDSS driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service or possibly have unspecified other impact via a large size value, related to mdss_compat_utils.c, mdss_fb.c, and mdss_rotator.c.	2016-08-30	10.0	CVE-2016-5344 CONFIRM CONFIRM

NVD Feed



National Cyber Awareness System

Vulnerability Summary for CVE-2016-5344

Original release date: 08/30/2016

Last revised: 08/31/2016

Source: US-CERT/NIST

Overview

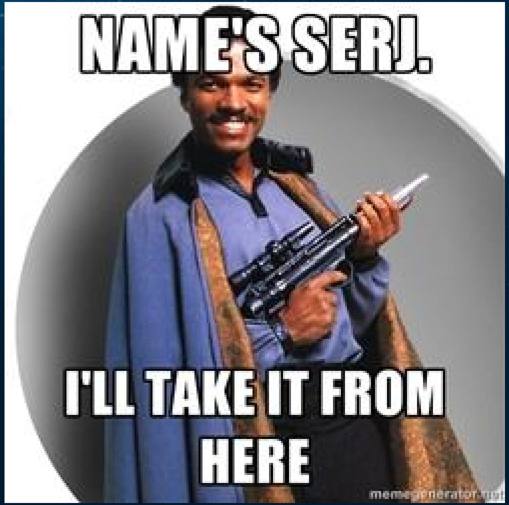
Multiple integer overflows in the MDSS driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service or possibly have unspecified other impact via a large size value, related to mdss_compat_utils.c, mdss_fb.c, and mdss_rotator.c.

Collecting CVEs - Under Development

```
rule linux_kernel_cve_2016_5344
{
strings:

    $cve = /[Cc][Vv][Ee][_-]? ?2016[_-]? ?5344/

condition:

    ($cve or tags contains "cve-2016-5344" or signatures contains "CVE-2016-5344") and
new_file and not tags contains "zero-filled"
}
```

Processing Hits - Under Development

1. When a rule is triggered, VT adds notification to list and is captured via API
2. Bot downloads the VT sample that triggered rule, if it meets the prioritization
3. Uploads to AMA for further analysis and grabs potential IOCs
4. Analysis takes it from there!



More Fun With Malware Analysis

DerbyCon 2016, Louisville, KY 9/21 - 9/25

VirusBulletin 2016, Denver 10/5 - 10/7

SecTor 2016, Toronto 10/18 - 10/19

www.ThreatConnect.com/blog

Questions?

@MalwareUtkonos

@ThreatConnect