Unlocking the Value of CVEs

By: @theroxyd

Vulnerability Management Service Architect

@Hurricane Labs

I Love Linux.

#1LinuxThingADay

Hurricane Labs

Today we’re talking about:

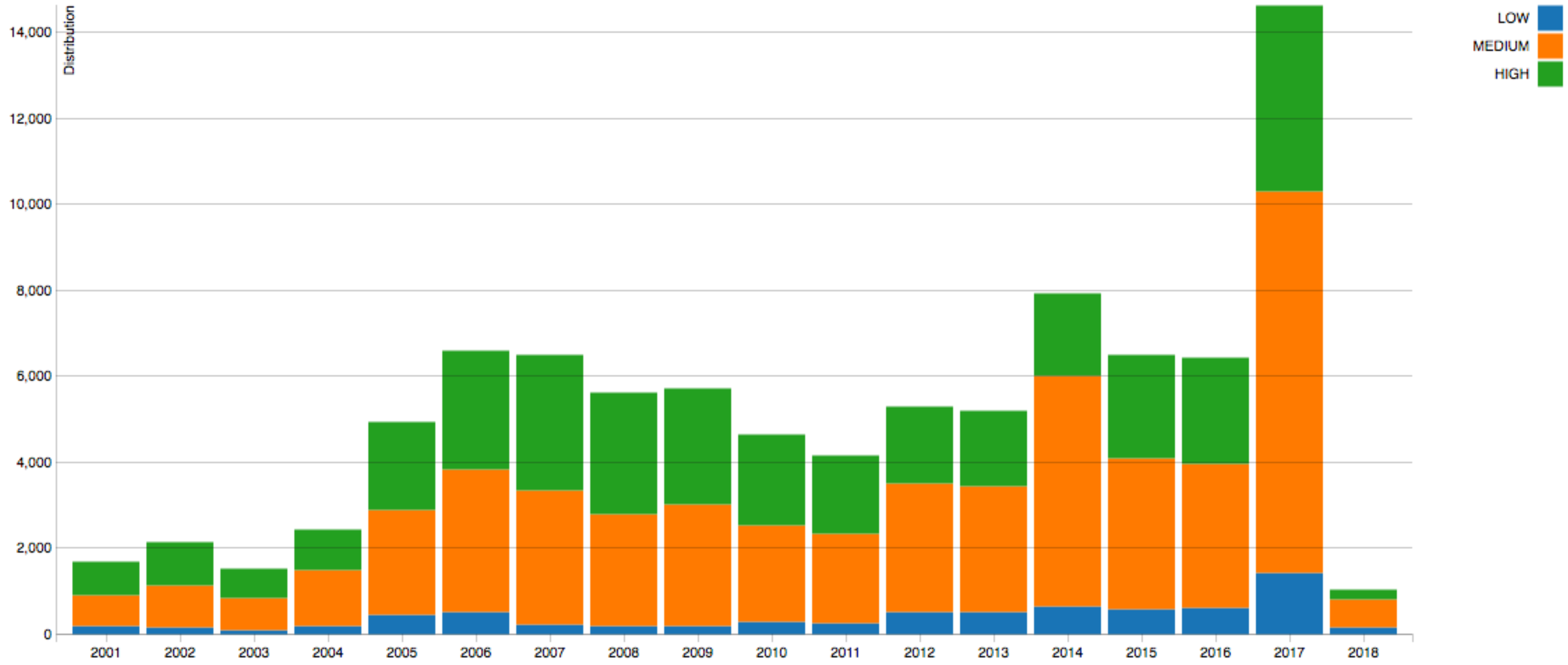
CVEs!

Information within Common Vulnerabilities & Exposures (CVEs) can be used to make vulnerability management easier and less scary.

No need to panic.

Hurricane Labs

Why don’t you just patch everything?



Source: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

cve-year-number

(year discovered OR the year assigned, whichever first)

description

cvss score

references

CVE-2017-11882 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11884.

Source: MITRE **Last Modified:** 11/14/2017 + View Analysis Description

QUICK INFO

CVE Dictionary Entry: CVE-2017-11882
Original release date: 11/14/2017
Last revised: 12/30/2017
Source: US-CERT/NIST

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 7.8 High
Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (legend)
Impact Score: 5.9
Exploitability Score: 1.8

CVSS Version 3 Metrics:

Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 HIGH
Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable - Victim must voluntarily interact with attack mechanism
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

Terminology

Vulnerability: Is a weakness that can be exploited

(Computational logic found in the software and/or hardware that hackers use to impact integrity or availability of system-critical data).

Exposure: Shows information that can be used in an attack

(Hackers use configuration "mistakes" as indirect stepping stones into your network to conduct information gathering or other hidden activities).

One’s not enough?
Try adding another.

Chaining: Combining a vulnerability with another one to create a larger effect (aka a problem).

C.I.A. Concepts

Confidentiality: Kept private - for authorized eyes only

Integrity: Unchanged - maintains the same meaning

Availability: Accessible - can be accessed and used as necessary

Access

Local: Must already have access (previously logged in or physically there).

Remote: May access or execute without being there or having prior access.

Terminology

Exploit: Used to take advantage of a vulnerability.

Zero-day: Exploit for a vulnerability that has no patch or fix.

Vulnerable Component: How the exploit gets in; what is being exploited.

Scope: Boundaries of what can be affected by the vulnerability.

Extra Credit!

Become familiar with common attacks.

owasp.org → attacks
Bonus round: read RFCs
(start with HTTP RFC 7230-7240)

CVSS Scores

BASE

EXPLOITABILITY; IMPACT; SCOPE

TEMPORAL

ENVIRONMENTAL

www.first.org/cvss/specification-document

Base Exploitability

Base score is one that does not change and remains consistent.

1. **Attack Vector** - network; adjacent; local; physical
2. **Attack Complexity** - low; high
3. **Privileges Required** - none; low; high
4. **User Interaction Required** - none; required

Attack Vector Network:

Access through network layer.

Attack Vector Adjacent:

Vulnerable component at network layer; limited to shared physical or logical network.

Exploitability

Hurricane Labs

Attack Vector Local:

Not at network stack; attacker must log in locally.

Attack Vector Physical:

Attacker has to be physically there.

Attack Complexity

Low:

“Attacker can expect repeatable success”

High:

Extra steps required

Privs Required

None: Unauthorized prior and during attack.

Low: Authorized with privileges affecting only settings by user.

High: Authorized w/privileges that give significant control.

User Interaction

None: No user interaction required.
Required: A user must complete an action.

Impact

High (total loss) ~ Low (some loss) ~ None

1. **Confidentiality**
2. **Integrity**
3. **Availability**

Scope

Changed or Unchanged

Could another component become vulnerable?

Temporal

Temporal score is one that can change over time.

1. Exploit Code Maturity
Not defined; high; functional; proof-of-concept; unproven

2. Remediation Level
Not defined; unavailable; workaround; temporary fix; official fix

3. Report Confidence
Not defined; confirmed; reasonable; unknown

Exploit Code Maturity

- **Not Defined:** Won’t affect score
- **High:** Functional; available; reliable
- **Functional:** Mostly works
- **Proof-of-concept:** Not practical/functional
- **Unproven:** No exploit code available

Remediation Level

- **Not Defined:** Won’t affect score
- **Unavailable:** No solution; impossible
- **Workaround:** Unofficial solution
- **Temporary Fix:** Not complete; from vendor
- **Official Fix:** Complete; from vendor

Report Confidence

- **Not Defined:** Won’t affect score
- **Confirmed:** Independently | author | vendor
- **Reasonable:** Can’t confirm; seems legit
- **Unknown:** Cause unknown or debateable

Environmental

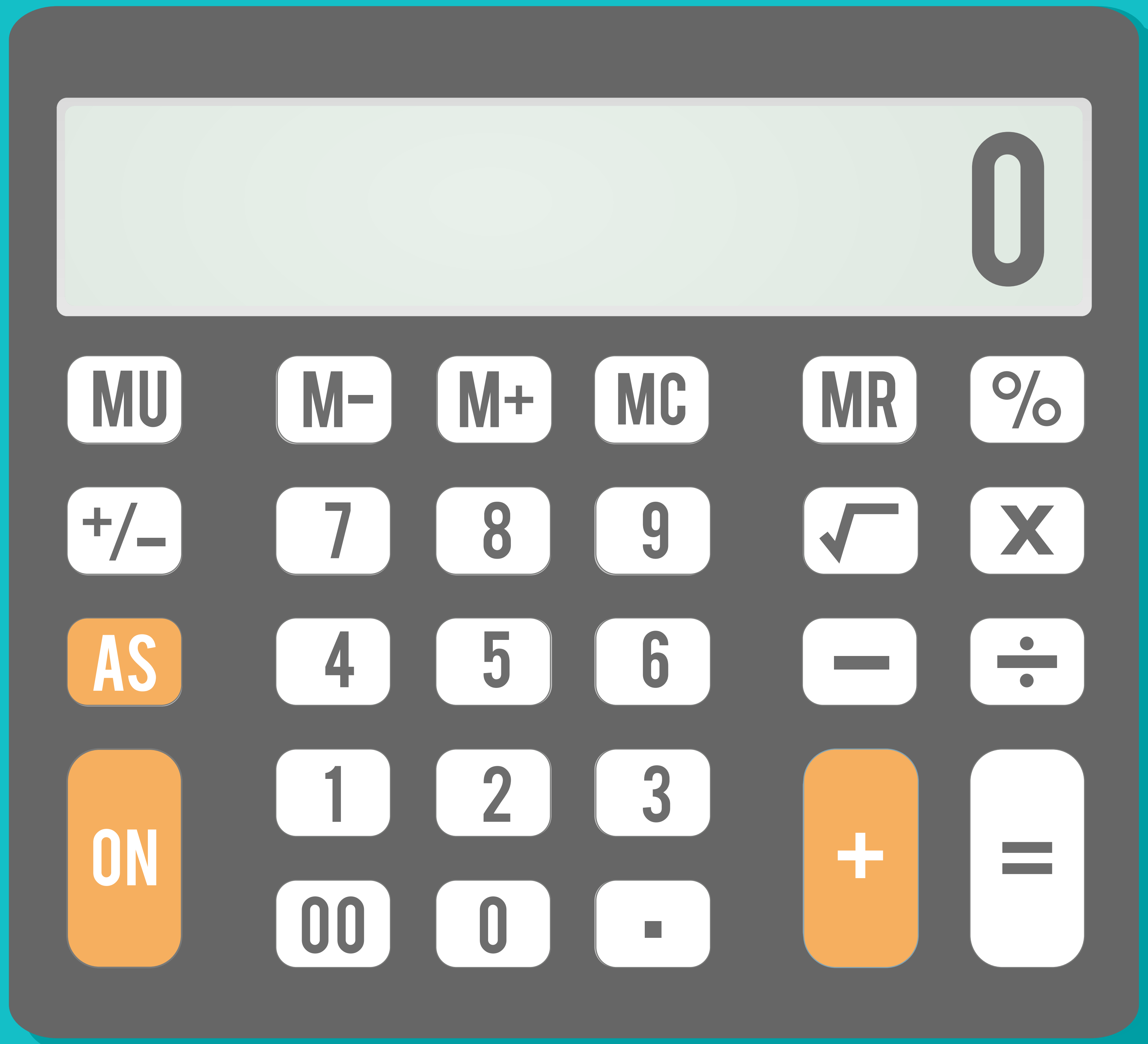
This is how you get a customized score.

1. Modified base metrics

2. Security requirements (CIA)
   - *What is the effect on each CIA?*
     Not defined; high; medium; low

use the calculator

first.org/cvss/calculator/3.0



Useful Tips

1. Filter out what isn’t applicable.

2. Automate.

3. Put it in a database.

4. Prioritize.

Useful Tips

5. Use workarounds and security controls.

6. Create reasonable deadlines.
(Don’t let remediation cause burnout.)

7. Put more detail in remediation plans.
(Use the references!)

Points to keep in mind

1. Response can be organized and actionable.

2. Not all vulnerabilities are scary - read the CVE!

Special thanks to:

Steve Christey Coley

(@sushidude)

Special thanks to:

Hurricane Labs

Q&A Time!

List of all my www things
Roxyd.github.io

Email me!
roxy@hurricanelabs.com