# Vulnerabilities and Patches


William P. Flinn

*M.S. Information Systems Security Management, CompTIA Security+, PatchLink Certified Engineer, PatchLink Certified Administrator*

Cyber-Security Analyst

Patching and Vulnerability Working Group Chair

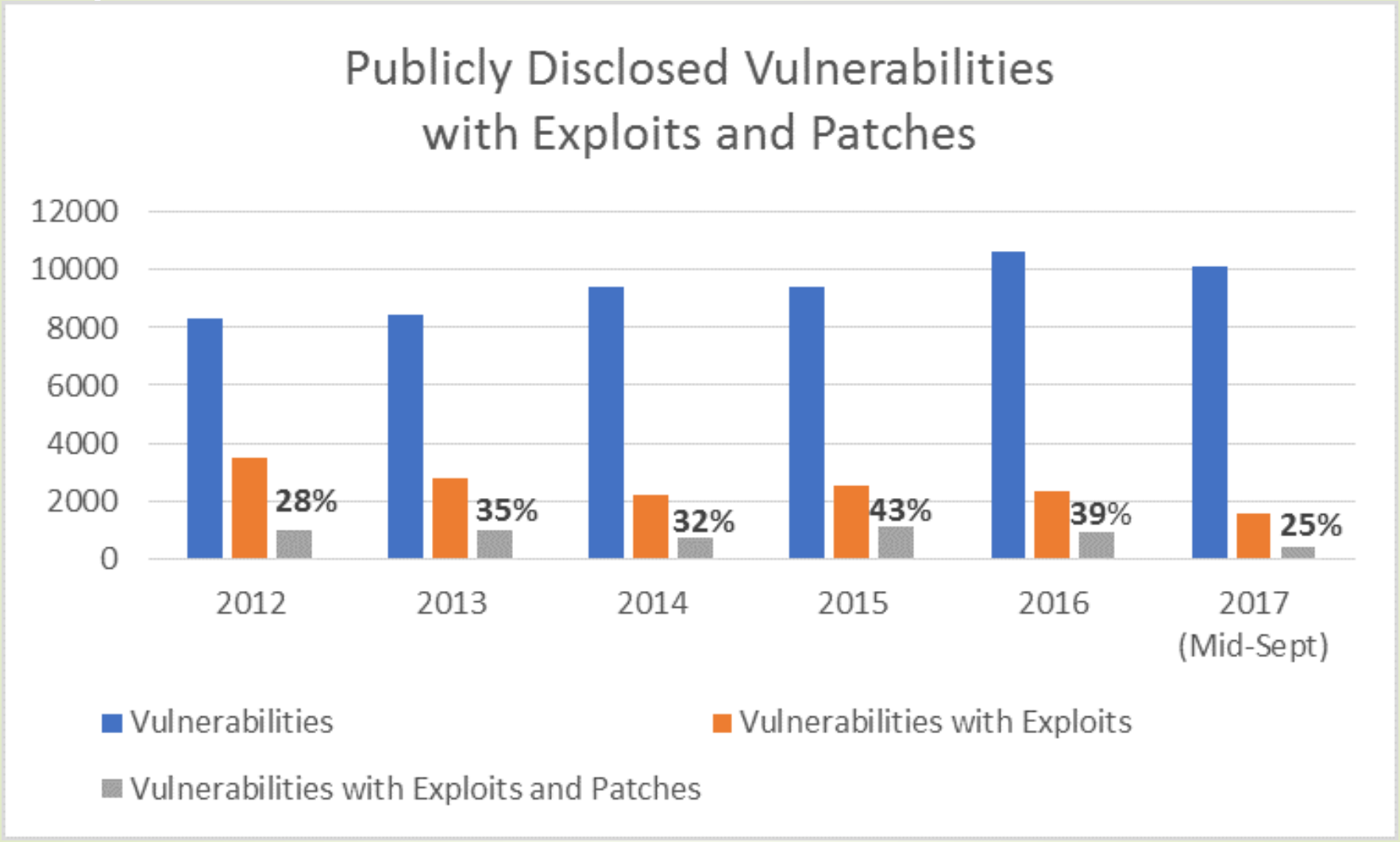
bill@gonzosgarage.net


# Vulnerability and Patching Concerns

- What are they?
- Why are there so many?
- If we are always deploying patches, why is our number of vulnerabilities seemingly not improving?
- If my computer is only missing one patch, why does it still have 76 vulnerabilities?!

# Vulnerability Terms and Definitions

- CPE
  - Common Platform Enumeration.
  - Formal name format for checking names against a system.
- CVE
  - Common Vulnerabilities and Exposures.
  - CVE numbers are unique identifiers for vulnerabilities.
  - CVE listing and statuses maintained by Mitre
- CVSS
  - Common Vulnerability Scoring System.
  - A scoring system to assign severity to vulnerabilities (CVEs).
  - Uses a base score, impact factors, exploitability factors, and "temporal" factors to determine final score.
- Patch
  - This is typically a software update for the operating system or for a software product installed on a computer.
  - A patch may address one or more vulnerabilities.
- Vulnerability
  - A weakness or flaw in a software or hardware component.
  - A vulnerability is a much more granular way to describe a single weakness in operating systems, software, or configurations.
  - One or more vulnerabilities can be remediated with a single patch.
- Exploit
  - Malicious software or other tool that takes advantage of a vulnerability


Publicly Disclosed Vulnerabilities with Exploits and Patches
12000
10000
8000
6000
4000
2000
0
28%
35%
32%
43%
39%
25%
2012
2013
2014
2015
2016
2017 (Mid-Sept)
Vulnerabilities
Vulnerabilities with Exploits
Vulnerabilities with Exploits and Patches

# CVSS Scoring System

## NVD Vulnerability Severity Ratings

NVD provides qualitative severity rankings of "Low", "Medium", and "High" for CVSS v2.0 base score ranges in addition to the severity ratings for CVSS v3.0 as they are defined in the CVSS v3.0 specification.

### CVSS v2.0 Ratings

| Severity | Base Score Range |
|---|---|
| Low | 0.0-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-10.0 |

### CVSS v3.0 Ratings

| Severity | Base Score Range |
|---|---|
| None | 0.0 |
| Low | 0.1-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-8.9 |
| Critical | 9.0-10.0 |

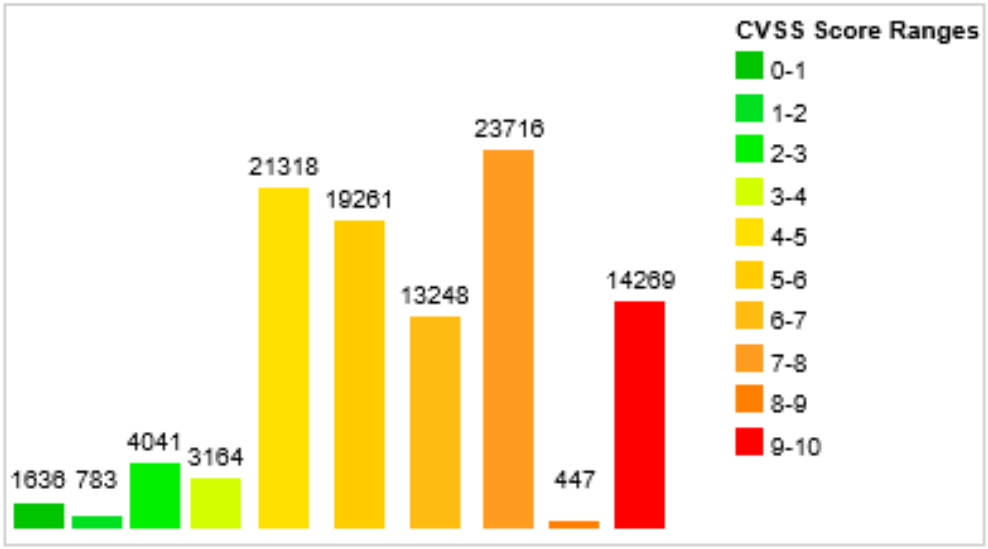
## Current CVSS Score Distribution For All Vulnerabilities

**Distribution of all vulnerabilities by CVSS Scores**

| CVSS Score | Number Of Vulnerabilities | Percentage |
|---|---|---|
| 0-1 | 1636 | 1.60 |
| 1-2 | 783 | 0.80 |
| 2-3 | 4041 | 4.00 |
| 3-4 | 3164 | 3.10 |
| 4-5 | 21318 | 20.90 |
| 5-6 | 19261 | 18.90 |
| 6-7 | 13248 | 13.00 |
| 7-8 | 23716 | 23.30 |
| 8-9 | 447 | 0.40 |
| 9-10 | 14269 | 14.00 |
| Total | 101883 | |

Weighted Average CVSS Score: **6.7**

**Vulnerability Distribution By CVSS Scores**



# CVSS Scoring Metrics

## Base Score Metrics

### Exploitability Metrics

**Attack Vector (AV)***

Network (AV:N) | Adjacent Network (AV:A) | **Local (AV:L)** | Physical (AV:P)

**Attack Complexity (AC)***

**Low (AC:L)** | High (AC:H)

**Privileges Required (PR)***

None (PR:N) | **Low (PR:L)** | High (PR:H)

**User Interaction (UI)***

**None (UI:N)** | Required (UI:R)

**Scope (S)***

**Unchanged (S:U)** | Changed (S:C)

### Impact Metrics

**Confidentiality Impact (C)***

None (C:N) | Low (C:L) | **High (C:H)**

**Integrity Impact (I)***

None (I:N) | Low (I:L) | **High (I:H)**

**Availability Impact (A)***

None (A:N) | Low (A:L) | **High (A:H)**

* - All base metrics are required to generate a base score.

## Temporal Score Metrics

**Exploitability (E)**

**Not Defined (E:X)** | Unproven that exploit exists (E:U) | Proof of concept code (E:P) | Functional exploit exists (E:F) | High (E:H)

**Remediation Level (RL)**

**Not Defined (RL:X)** | Official fix (RL:O) | Temporary fix (RL:T) | Workaround (RL:W) | Unavailable (RL:U)

**Report Confidence (RC)**

**Not Defined (RC:X)** | Unknown (RC:U) | Reasonable (RC:R) | Confirmed (RC:C)

# CVSS Scoring Metrics

## Environmental Score Metrics

### Base Modifiers

**Attack Vector (AV)**

Not Defined (MAV:X) | Network (MAV:N) | Adjacent Network (MAV:A) | Local (MAV:L) | Physical (MAV:P)

**Attack Complexity (AC)**

Not Defined (MAC:X) | Low (MAC:L) | High (MAC:H)

**Privileges Required (PR)**

Not Defined (MPR:X) | None (MPR:N) | Low (MPR:L) | High (MPR:H)

**User Interaction (UI)**

Not Defined (MUI:X) | None (MUI:N) | Required (MUI:R)

**Scope (S)**

Not Defined (MS:X) | Unchanged (MS:U) | Changed (MS:C)

### Impact Metrics

**Confidentiality Impact (C)**

Not Defined (MC:X) | None (MC:N) | Low (MC:L) | High (MC:H)

**Integrity Impact (I)**

Not Defined (MI:X) | None (MI:N) | Low (MI:L) | High (MI:H)

**Availability Impact (A)**

Not Defined (MA:X) | None (MA:N) | Low (MA:L) | High (MA:H)

### Impact Subscore Modifiers

**Confidentiality Requirement (CR)**

Not Defined (CR:X) | Low (CR:L) | Medium (CR:M) | High (CR:H)

**Integrity Requirement (IR)**

Not Defined (IR:X) | Low (IR:L) | Medium (IR:M) | High (IR:H)

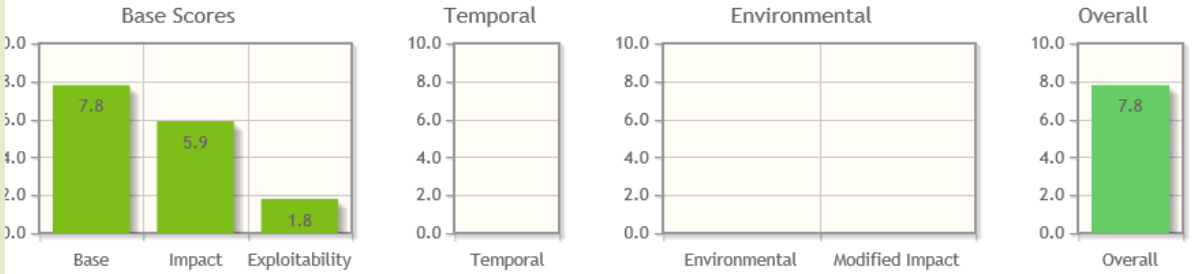
**Availability Requirement (AR)**

Not Defined (AR:X) | Low (AR:L) | Medium (AR:M) | High (AR:H)

# CVSS Scoring Example

## Common Vulnerability Scoring System Calculator Version 3 CVE-2016-0051

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.




**CVSS Base Score:** 7.8
Impact Subscore: 5.9
Exploitability Subscore: 1.8
**CVSS Temporal Score:** NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
**Overall CVSS Score:** 7.8

Show Equations

**CVSS v3 Vector**

AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

# Vulnerability and Patch Relationships

- What's The Difference?
  - Where a patch is an update that addresses several vulnerabilities, a vulnerability, in contrast, is a single security weakness.
  - The short story is that a patch typically addresses one or more vulnerabilities. The vulnerability is the "hole," and the patch is a "fix."
  - But not all vulnerabilities are remediated with patches.
    - Configuration settings such as turning off BlueTooth.
    - Removing old, vulnerable software.
    - Removing outdated and non-secure protocols and services.
    - A patch does not yet exist – may have to use other compensating measures or workarounds.

# Vulnerability versus Patch Example:

- When the Adobe Acrobat 11.0.16 update was released, it provided remediation for 76 different vulnerability CVE items that were rated as HIGH in the CVSS v2 scoring system.

- After deploying this and other patches to the 9,000 computers that needed the update, and then performing an analysis of the residual vulnerabilities a few days after the deployments started, we found that 7,500 computers received the Acrobat patch, but 1,500 computers were still unpatched for this specific patch.

- In patching terms, we are showing 83% patched for Adobe Acrobat 11.0.16 in the patch status reports, which is pretty good progress after only a few days.

- In a vulnerability report a few days after deployments started, however, we still showed as having over 120,000 High CVSS vulnerabilities.

- This ONE MISSING PATCH on those 1,500 computers (17% of the total number of computers needing the patch) accounts for 114,000 vulnerability line items of the approximately 120,000 on the report.

# Vulnerability versus Patch Example:

| | |
|---|---|
| **Fixlet Name:** | Adobe Acrobat Reader DC 2018.011.20040 Available - Adobe Acrobat Reader DC - Continuous Track |
| **Sitename:** | Updates for Windows Applications |
| **Fixlet ID:** | 8101235 |
| **Category:** | Security Update |
| **Download Size:** | 98.57 MB |
| **Source:** | Adobe |
| **Source ID:** | APSB18-09 |
| **Source Release Date:** | 5/14/2018 |
| **Source Severity:** | Critical |
| **CVE:** | CVE-2018-4947; CVE-2018-4948; CVE-2018-4949; CVE-2018-4950; CVE-2018-4951; CVE-2018-4952; CVE-2018-4953; CVE-2018-4954; CVE-2018-4955; CVE-2018-4956; CVE-2018-4957; CVE-2018-4958; CVE-2018-4959; CVE-2018-4960; CVE-2018-4961; CVE-2018-4962; CVE-2018-4963; CVE-2018-4964; CVE-2018-4965; CVE-2018-4966; CVE-2018-4967; CVE-2018-4968; CVE-2018-4969; CVE-2018-4970; CVE-2018-4971; CVE-2018-4972; CVE-2018-4973; CVE-2018-4974; CVE-2018-4975; CVE-2018-4976; CVE-2018-4977; CVE-2018-4978; CVE-2018-4979; CVE-2018-4980; CVE-2018-4981; CVE-2018-4982; CVE-2018-4983; CVE-2018-4984; CVE-2018-4985; CVE-2018-4986; CVE-2018-4987; CVE-2018-4988; CVE-2018-4989; CVE-2018-4990; CVE-2018-4993; CVE-2018-4995; CVE-2018-4996 |
| **SANS:** | SANS C2 |
| **First detected:** | 2018-05-18 04:44:37 |

# Vulnerability Scanning and Patch Remediation Challenges:

- False positives.
- False negatives (the unknown unknowns).
- Patching system or agent malfunctions.
- Users who work in the field and do not connect regularly to get updates or to get scanned.
- Old and vulnerable software that leaves "leftovers" on the endpoint, even after removal.
  - If the bits are on the box, you must remediate!
- Disagreement between assessment tools.

# What YOU Can Do…

- Form a Patching and Vulnerability Working Group to analyze patching requirements and vulnerability remediation effectiveness.
- Perform regular vulnerability scanning and assessment with multiple tools (Nessus, IBM SCA)
- Implement a centralized patch management system, such as Lumension, Tivoli, or SCCM/WSUS, and ensure that your centralized patch management agents are installed and running properly.
- Enforce agent installation through Group Policy Objects (GPOs), or tools like ForeScout/Counteract.
- Ensure that your end users, especially remote users, connect their computers to your network or VPN regularly to get scanned, receive configuration policies and patches, and then again to report their patch status.
- Ensure that only needed and authorized products, protocols, and services are installed on your computers.
- Sign up for various vendor, US-CERT, SANS, and other regular vulnerability notifications.

# Wrapping It All Up!

- Patching and vulnerability management are vital processes in any organization's overall cyber-security program.
- Ensuring that all security software is installed and running is vital to this process.
- Make sure that computers are receiving their patch updates, and unnecessary software and services are not running on computers.
- Performing regular patching is important, but so is doing meaningful follow up analysis.
- Find out where your "holes" are, find out what the "plugs" are for those holes, prioritize the weaknesses, and get 'em fixed!

# References

- NIST National Vulnerability Database (NVD) Home:
  - https://nvd.nist.gov/home
- NIST NVD, CVSS Scoring System
  - https://nvd.nist.gov/vuln-metrics/cvss
- NIST NVD, CVSS v3 Calculator:
  - https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- CVSS Standards/User Guide:
  - https://www.first.org/cvss/user-guide
- Mitre CVE List Home:
  - https://cve.mitre.org/cve/
- CVE Numbering Authorities:
  - https://cve.mitre.org/cve/cna.html
- NIST NVD CPE Dictionary:
  - https://nvd.nist.gov/products/cpe
- DHS US-CERT National Cybersecurity and Communications Integration Center:
  - https://www.us-cert.gov/

# Questions/Discussion