The Life of a Bug Report

by Brian Schweigler

Bachelor Thesis, 1st presentation

15th October 2019
Motivation

«One does not know all the expected effects of known bugs.»

— Frederick Brooks, The Mythical Man-Month
What is a good bug report?

The Art of Bug Reporting

- Place the bug details in a highly visible area
- Describe the bug accurately so others would recognise it
- Include the time and date of the bug find
- Explain the location and environment where the bug dwells
- Highlight how damaging or dangerous the bug is
- Give a brief summary of the bug
- Detail how to find the bug again and what footprints to follow
From a bug to the attack

Bug
Problem caused by code that produces an unexpected result.

Vulnerability
Bug that allows attackers to carry out prohibited actions.

Exploit
Executable code that leverages the vulnerability.

Attack
Propagation of vulnerability reports

users / developers / companies

CVE
Common Vulnerability & Exposures

NVD
National Vulnerability Database

Rapid7

Exploit DB

CX SECURITY

snyk

VulDB
Preliminary research questions

RQ1:
What are the commonly used criteria in bug reports, and how are they used?

RQ2:
How and when are reports propagated between the various databases? Can we find any trends?

RQ3:
What is the role and reliability of the used vulnerability score metrics?
### Notable observation #1

**RQ1** (Criteria): Missing data

---

**ACTi ACM-3100 Camera Remote Command Execution**

<table>
<thead>
<tr>
<th>Date</th>
<th>Risk</th>
<th>Local</th>
<th>Remote</th>
<th>CVE</th>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019.09.26</td>
<td>High</td>
<td>No</td>
<td>Yes</td>
<td>N/A</td>
<td>CWE-78</td>
</tr>
</tbody>
</table>

**Credit:** Todor Donev

**significance?**
RQ1 (Criteria)

Notable observation #2

Harmful data

Availability of

Proof-of-Concept? Exploit?

 CVE-2019-16701

CVE-2019-16701

Learn more at National Vulnerability Database (NVD)

- CVSS Severity Rating
- Fix Information
- Vulnerable Software Versions
- SCAP Mappings
- CVE Information

Description

pfsense through 2.3.4 through 2.4.4-p3 allows Remote Code Injection via a methodCall XML document with a pfense.exe_call_xml call containing shell metacharacters in a parameter value.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:http://n课外安全.com/154587/efSense-2.3.4-2.4.4-p3-Remote-Code-Injection.html
- MISC:https://github.com/pfense/pfense/commits/master

Exploit?

Availability of

Proof-of-Concept?
RQ2 (Propagation) Notable observation #3

Information leak before «official» disclosure

<table>
<thead>
<tr>
<th>CVE-ID</th>
<th>Description</th>
<th>Severity</th>
<th>CVSS</th>
<th>Published</th>
<th>Created</th>
<th>Added</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2019-8772</td>
<td>This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.</td>
<td>4</td>
<td>(AV:L/AC:M/Au:N/C:P/I:P/A:P)</td>
<td>10/08/2019</td>
<td>10/09/2019</td>
<td>10/08/2019</td>
<td>10/08/2019</td>
</tr>
</tbody>
</table>

OS X update for PDFKit (CVE-2019-8772)

An issue existed in the handling of links in encrypted PDFs. This issue was addressed by adding a confirmation prompt.
RQ2 (Propagation) Notable observation #4

Information leak before «official» disclosure

Android - Binder Driver Use-After-Free

**CVE-ID**

**CVE-2019-2215** Learn more at National Vulnerability Database (NVD)

- CVSS Severity Rating
- Fix Information
- Vulnerable Software Versions
- SCAP Mappings
- CPE Information

**Description**

**RESERVED** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

The following issue exists in the android-msm-wahoo-4.4-pie branch of https://android.googlesource.com/kernel/msm (and possibly...
Notable observation #5

Scores diverge
Next Steps

1. **Download or parse** data from vulnerability database websites

2. **Reverse bug report look ups** to collect initial reports from accessible repositories

3. **Search** within the data for outliers and trends

4. **Distill findings for advice** towards developers, security researchers & end users
Summary

Unstructured & distributed information

Solution

Vision
Sources

• “Ladybird Clipart”, Meladee

• “The Art of Bugreporting”, Andy Glover
  http://cartoontester.blogspot.com/

• Sources for definitions and background information (Slide 4)
  https://www.kb.cert.org/vuls/guidance/ 09.10.19 (18:00)
  https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/ 09.10.19 (18:00)
  https://www.gizmosphere.org/network-security-vulnerabilities-vs-exploits/ 09.10.19 (18:00)