WITHYOU WITHME

CVSS Capstone Briefing

CVE-2009-0658

Name : Phillip Newlove
Date: 13/12/23

WITHYOU WITHME

Scope

This briefing will cover a detailed breakdown of the CVSS score for CVE-2009-0658 in order to understand what the scoring means and how it was achieved.

My name is Phillip Newlove (Phil), I am a student of WYWM, I created the CVSS score and I will be explaining how and why I did each step.

WITHYOU WITHME

Threat

CVE-2009-0658 Detail

Description

Buffer overflow in Adobe Reader 9.0 and earlier, and Acrobat 9.0 and earlier, allows remote attackers to execute arbitrary code via a crafted PDF document, related to a non-JavaScript function call and possibly an embedded JBIG2 image stream, as exploited in the wild in February 2009 by Trojan.Pidief.E.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.8 HIGH **Vector:** CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

WITHYOU WITHME

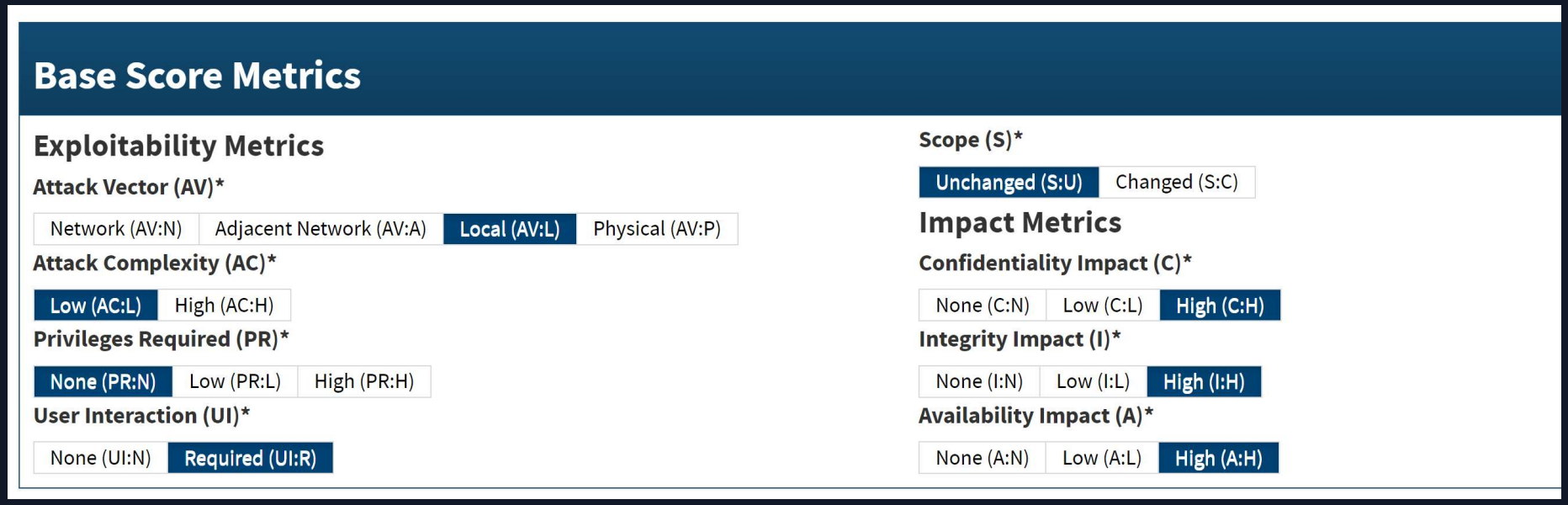
Threat Cont'd

CVE-2009-0658 is a buffer overflow vulnerability in Adobe Reader versions 9.0 and earlier. This allows arbitrary code to be executed on the system via a malicious PDF document that is opened by the user.

References - https://nvd.nist.gov/vuln/detail/CVE-2009-0658

WITHYOU WITHME

Base Score 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)**

Base Score : **7.8**

WITHYOU WITHME

Base Score Metrics Cont'd

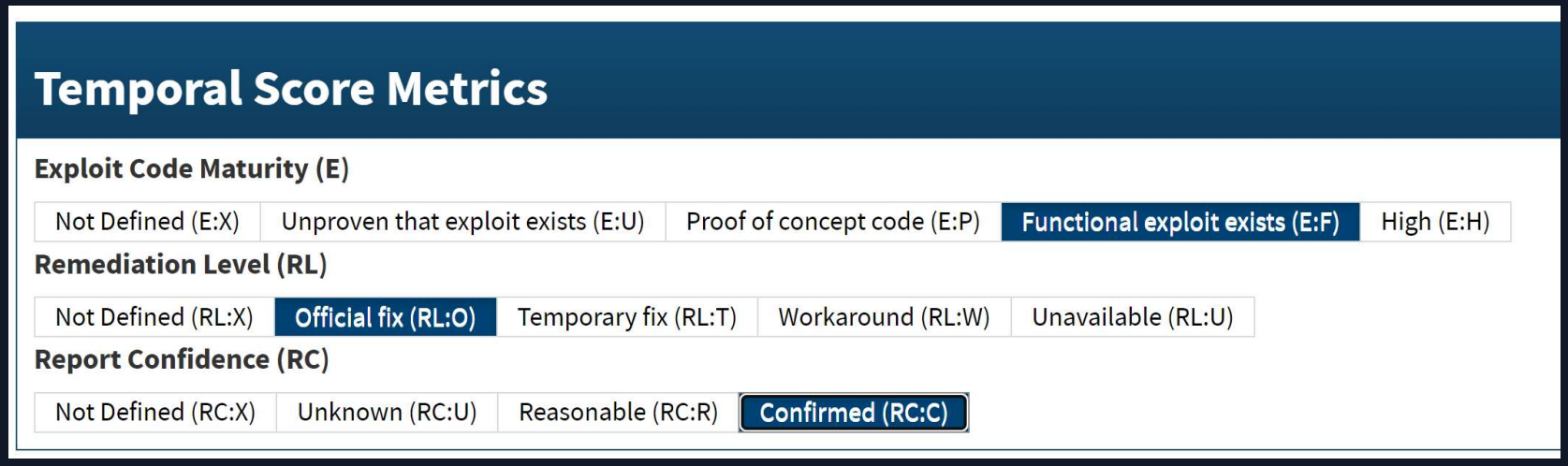
I found the base score to be 7.8. This was based on:

- Attack Vector : Local – I concluded this was a local attack vector since the exploit relied on uploading a file to the victim's computer, which then had to be opened by a user locally.
- Attack Complexity : Low – I scored this as low attack complexity since the only action required to trigger the exploit, is the user opening the malicious file.
- Privileges Required : None – The attack requires no privileges from the attacker's side, only the ability to send a file.
- User Interaction : Required – The exploit requires the user to open the malicious file.
- Scope : Unchanged – The arbitrary code executed on the target is dependent upon the privileges of the user that is exploited, resources out of reach of the user are also out of reach of the attacker.

Impact metrics – Confidentiality, Integrity and Availability all have a high chance of being impacted, depending on the target user's privileges.

WITHYOU WITHME

Temporal Score Metrics



Temporal Score : **7.2**

WITHYOU WITHME

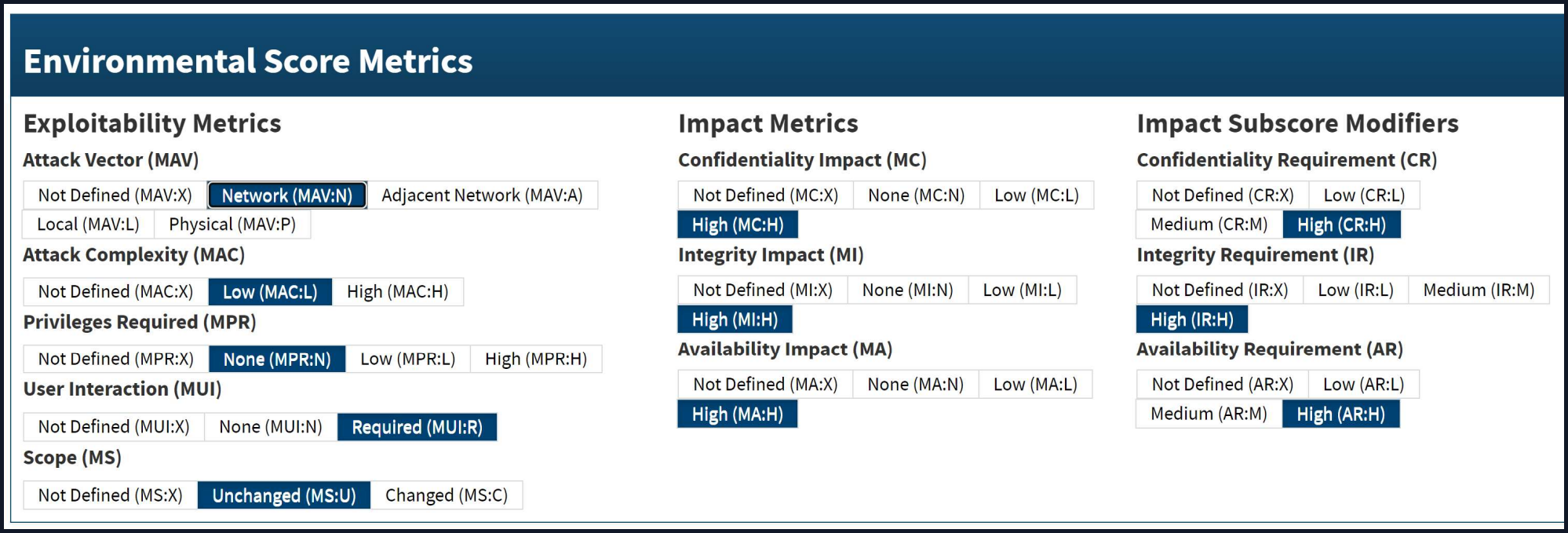
Temporal Score Metrics Cont'd

I found the Temporal score to be 7.2. This was based on:

- Exploit Code Maturity : Functional Exploit Exists – There are functional exploits on exploitDB (including Metasploit modules) (https://www.exploit-db.com/)
- Remediation Level : Official Fix – Adobe have released an updated version of Acrobat and Reader to resolve this vulnerability (https://www.adobe.com/support/security/advisories/apsa09-01.html)
- Report Confidence : Confirmed – There are multiple sources (including from the vendors themselves) detailing the vulnerability and its exploits (https://www.exploit-db.com/), (https://www.adobe.com/support/security/advisories/apsa09-01.html), (https://nvd.nist.gov/vuln/detail/CVE-2009-0658)

WITHYOU WITHME

Environmental Score Metrics



Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

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

Attack Complexity (MAC)

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

Privileges Required (MPR)

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

User Interaction (MUI)

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

Scope (MS)

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

Impact Metrics

Confidentiality Impact (MC)

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

Integrity Impact (MI)

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

Availability Impact (MA)

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)**

Environmental Score : **8.2**

WITHYOU WITHME

Environmental Score Metrics Cont'd

I found the Environmental score to be 8.2. This was based on:

- Attack Vector : Network – The malicious file is transferred across network boundaries and the code can be executed remotely.
- Attack Complexity : Low – The only requirement for the attack to work is that the victim has a vulnerable Adobe version, then they download and open the file.
- Privileges Required : None – The attacker is unauthorised and requires no access to settings or files.
- User Interaction : Required – The user must download and open the file for the exploit to work.
- Scope : Unchanged - The arbitrary code executed on the target is dependent upon the privileges of the user that is exploited, resources out of reach of the user are also out of reach of the attacker.

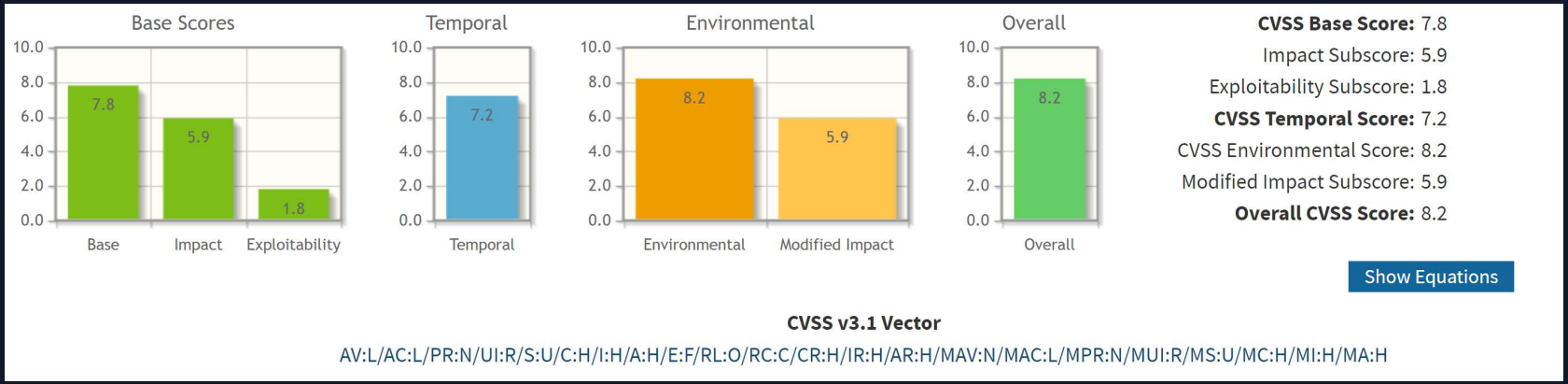
Impact Metrics – Confidentiality, Integrity and Availability all have a high chance of being impacted, depending on the target user's privileges.

Impact Subscore Modifiers – Should an attacker launch a successful exploit against a privileged user, the impact to the business and its employees Confidentiality, Integrity and Availability could be severe and catastrophic.

WITHYOU WITHME

Overall Score

I found the overall score to be 8.2, this was taken from a combination of the base, temporal and environmental scores.



Overall Score : **8.2**

WITHYOU WITHME

Recommendations

To remediate vulnerability to this exploit I recommend:

1. Upgrade to Adobe reader and acrobat versions 9.1 or greater.
2. Update virus definitions
3. Exercise caution when receiving and opening PDF documents

If an attacker compromises a user with high level privileges (Administrator), this could enable them total and unrestricted access to all business, customer and employee data.

WITHYOU WITHME

Conclusion

To summarise, we discussed:

- What CVE-2009-0658 is and how it can affect a victim
- The CVSS score, what it means and how it was created.
- My recommendations to reduce the risk of an attack.

WITHYOU WITHME

Questions?