1.1

e) Was für ein Verwundbarkeitstyp ist Heartbleed laut CWE?

CWE-126: Buffer Over-read

- Entsteht, wenn eine Anwendung versucht, Daten von einem Puffer oder Speicherbereich zu lesen, der kleiner ist als die angeforderte Datenmen
- Führt dazu, dass die Anwendung auf Speicher zugreift, der außerhalb des zugewiesenen Bereichs liegt und möglicherweise Daten liest, die nicht für sie vorgesehen sind
    - Kann zu unerwartetem Verhalten, einschließlich Abstürzen oder Sicherheitslücken führen

f) Lernen Sie weitere Details zu Heartbleed, bspw. hinsichtlich Gegenmaßnahmen, Exploits, betroffener Software und ähnlichen Verwundbarkeiten.

- Betroffene Software: Heartbleed betraf die OpenSSL-Bibliothek, die von vielen Webservern, E-Mail-Servern, VPN-Gateways und anderen Netzwerkdiensten verwendet wird.

- Gegenmaßnahmen:

    - Als Unternehmen/Seitenbetriber: Um gegen Heartbleed geschützt zu sein, mussten betroffene Organisationen schnell reagieren, indem sie ihre OpenSSL-Versionen auf eine nicht anfällige Version aktualisierten.
    - Als Entwickler: eine if-Abfrage

- Exploits

    - Entschlüsselung archivierter Daten
    - Entschlüsselung während der Webserver-Verbindungsaufnahme
    - Entschlüsselung der Verbindungsaufnahme an VoIP-Telefonen, Netzwerkdruckern und Routern

- Ähnliche Schwachstellen, wie Heartbleed, die auf unsicheren Speicheroperationen beruhen:

    - "Buffer Overflow"-Schwachstelle
        - Schwachstelle, die auftritt, wenn ein Programm versucht, mehr Daten in einen Puffer oder Speicherbereich zu schreiben, als dieser aufnehmen kann.
    - "Catastrophic Backtracking" in OpenSSL (CVE-2015-0291),
        - ermöglichte Angreifern, den SSL-Server durch Senden eines speziell gestalteten Pakets zum Absturz zu bringen

1.2

a) Um welche Verwundbarkeit handelt es sich genau? Um welchen Verwundbarkeitstyp han- delt es sich?

Die Schwachstelle mit der CVE-2017-5754 wird auch als Meltdown bezeichnet und betrifft Prozessoren von Intel sowie einige ARM- und IBM-Power-Prozessoren. Es handelt sich bei dieser Schwachstelle um eine Hardware-Schwachstelle, die aufgrund eines Designfehlers in der Prozessorarchitektur entstanden ist.

b) Was ist die Ursache der Verwundbarkeit und wie kann sie ausgenutzt werden?

Die Ursache für die Schwachstelle CVE-2017-5754, auch bekannt als Meltdown, liegt in der Art und Weise, wie moderne Prozessoren Speicherzugriffe optimieren, um eine höhere Leistung zu erzielen. Aufgrund dieser Optimierungen werden Speicherzugriffe teilweise vor der Berechtigungsprüfung durchgeführt, was es einem Angreifer ermöglicht, vertrauliche Informationen auszulesen, auf die er normalerweise keinen Zugriff hätte.

Ein Angreifer kann diese Schwachstelle ausnutzen, indem er einen speziell präparierten Programmcode ausführt, der es ihm erlaubt, den Inhalt des Speichers auszulesen, der normalerweise für andere Prozesse oder das Betriebssystem zugänglich ist. Durch die Ausnutzung dieser Schwachstelle kann ein Angreifer vertrauliche Informationen wie Passwörter, Kryptoschlüssel oder andere sensible Daten auslesen.

Es ist wichtig zu beachten, dass ein Angreifer bereits Zugriff auf das System haben und speziell präparierten Code ausführen muss, um diese Schwachstelle auszunutzen.

c) Welche Produkte sind von der Verwundbarkeit betroffen?

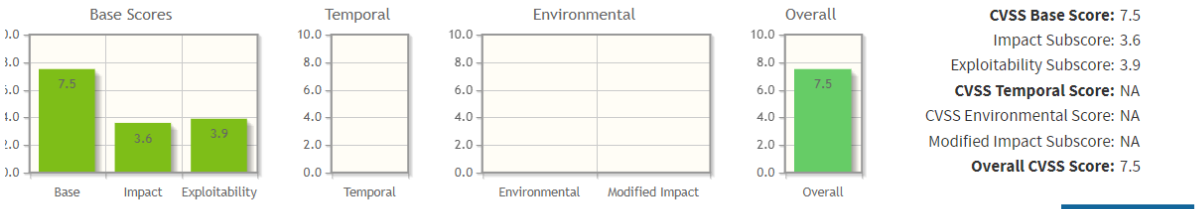
Die Schwachstelle betrifft hauptsächlich Prozessoren von Intel sowie einige ARM- und IBM-Power-Prozessoren, die seit 1995 entwickelt wurden. Die Schwachstelle wurde im Januar 2018 öffentlich bekannt gemacht und wurde als eine der schwersten Sicherheitslücken in der Geschichte der IT-Industrie eingestuft.

d)

e) Berechnen Sie den CVSS Score mit dem "Common Vulnerability Scoring System Calcu- lator Version 3.1". Welche qualitativen Unterschiede zum CVSS 3.1 Score von Heartbleed k¨onnen Sie dabei feststellen?

Common Vulnerability Scoring System Calculator

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: 7.5
Impact Subscore: 3.6
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.5

Show Equations

CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

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)

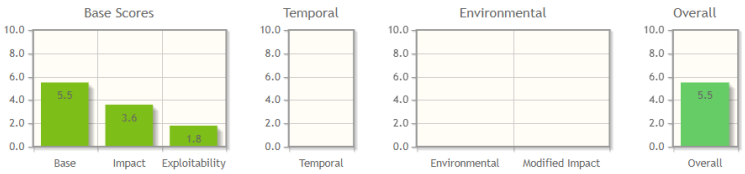
Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

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

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

Common Vulnerability Scoring System Calculator

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: 5.5
Impact Subscore: 3.6
Exploitability Subscore: 1.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 5.5

Show Equations

CVSS v3.1 Vector
AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

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)