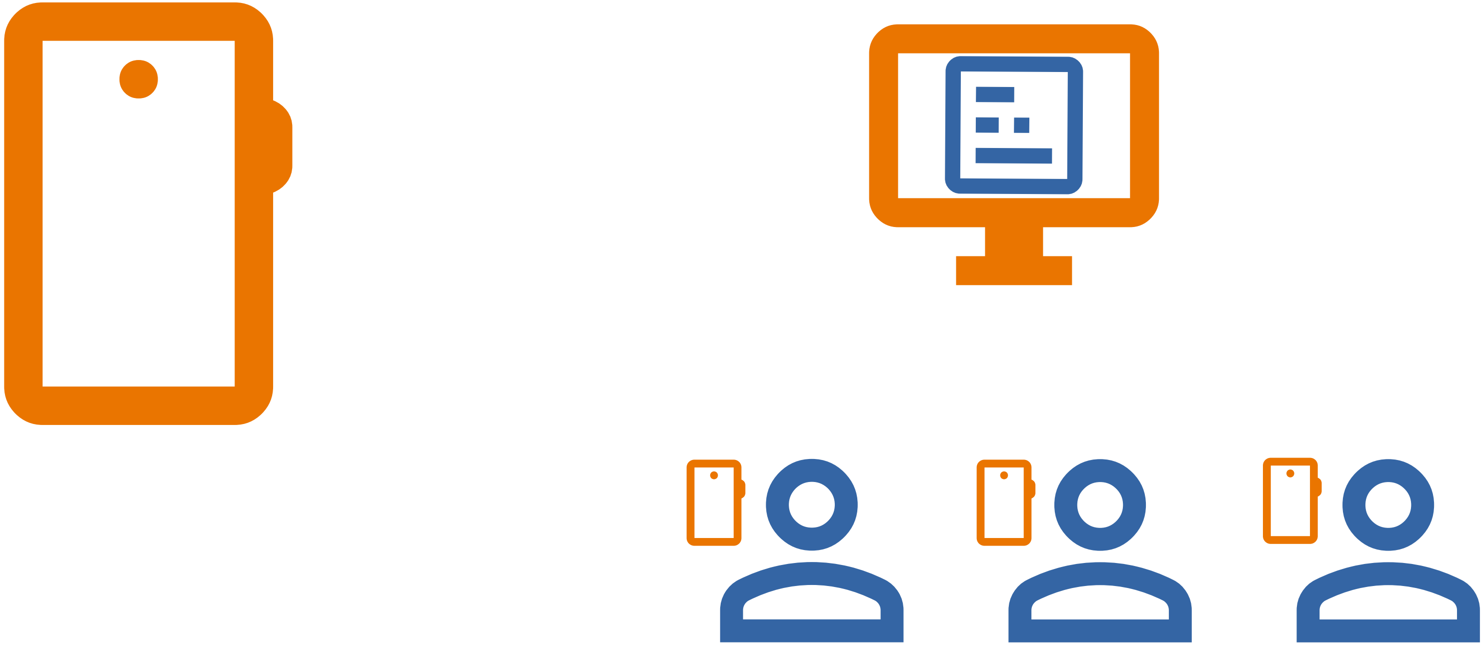
Scoring Vulnerabilities using CVSS

Martin Georgiev

OWASP
SOFIA, BULGARIA



CVSS

Common Vulnerability Scoring System

Open framework for communicating the characteristics and severity of vulnerabilities

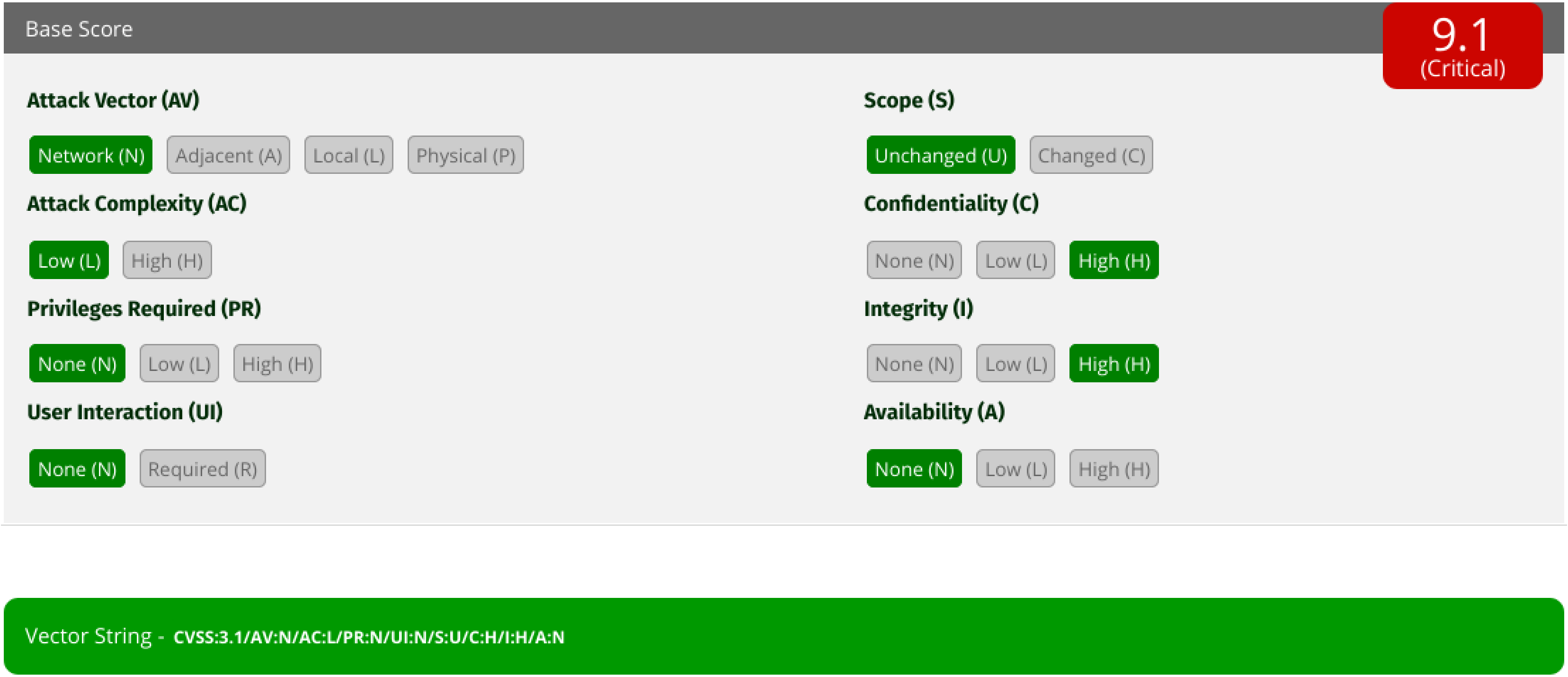
CVSS is not CVE

https://www.first.org/cvss/

CVSS Score	Rating
9.0 – 10.0	Critical
7.0 – 8.9	High
4.0 – 6.9	Medium
0.1 – 3.9	Low
0.0	None

CVSS

Tells us a story



Base Score

9.1
(Critical)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

[✓ None (N)] Low (L) High (H)

Vector String - **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N**

CVSS is not a Risk Score

vs

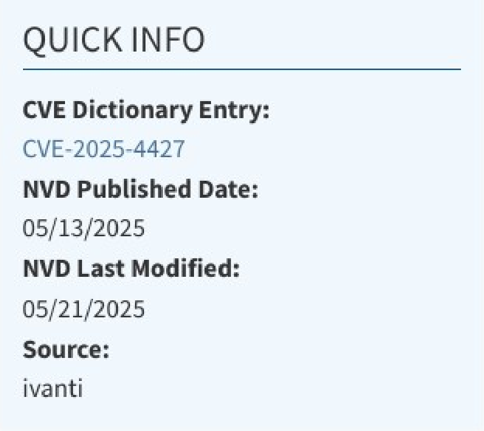
CVSS

CVSSv3.1 vs CVSSv4.0

- CVSSv4 still not yet fully adopted
- Switching from CVSSv3 to CVSSv4 is a small step

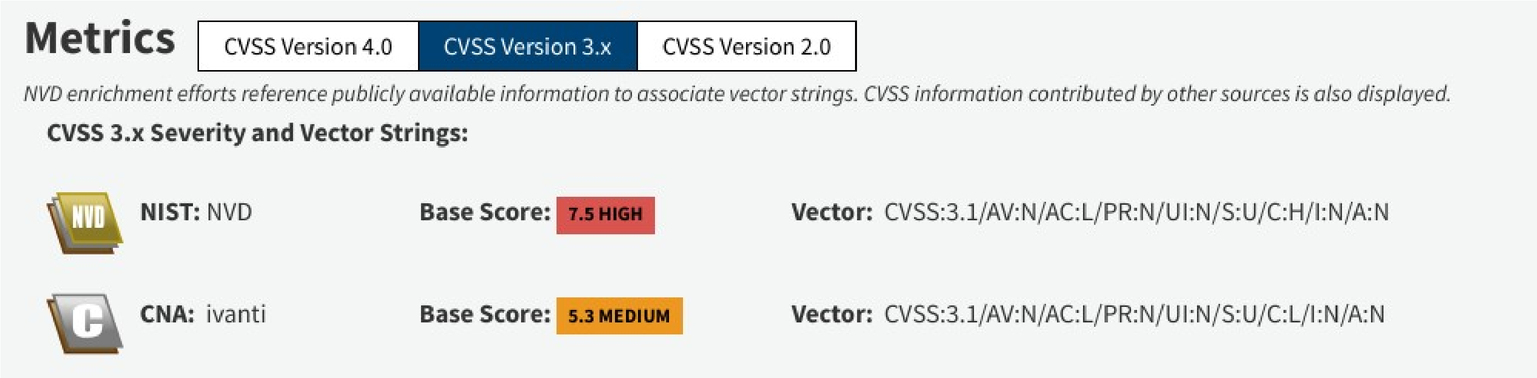
CVSS

CVE-2025-4427



QUICK INFO

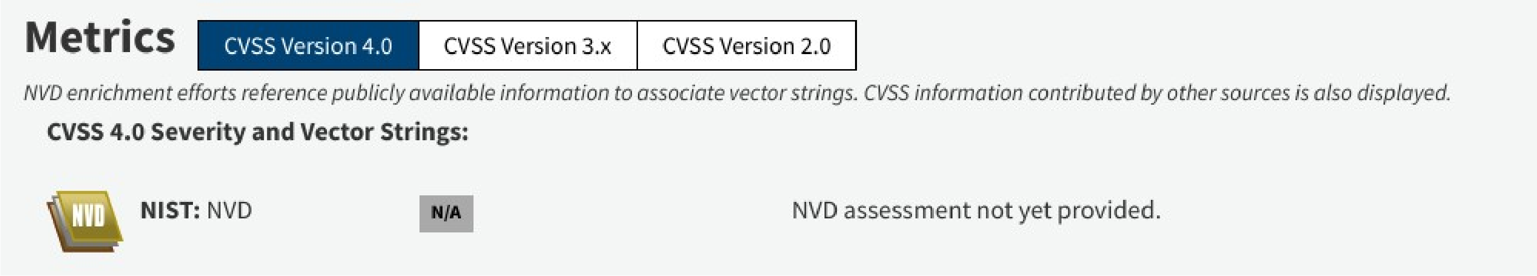
CVE Dictionary Entry:
CVE-2025-4427
NVD Published Date:
05/13/2025
NVD Last Modified:
05/21/2025
Source:
ivanti



NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD	**Base Score:** 7.5 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CNA: ivanti	**Base Score:** 5.3 MEDIUM	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N



NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 4.0 Severity and Vector Strings:

NIST: NVD	N/A	NVD assessment not yet provided.

https://nvd.nist.gov/vuln/detail/cve-2025-4427

CVSSv3.1

CVSS

Metrics

Groups

- Base
- Temporal
- Environmental

CVSS

Metrics

Groups

- Base
- Temporal
- Environmental

Base Score

- Intrinsic characteristics
- Constant over time
- Assumes reasonable worst-case impact across deployed environments

CVSS

Metrics

Groups

- Base
- Temporal
- Environmental

Temporal Score

Factors change over time

- Exploit Code Maturity
- Remediation Level
- Report Confidence

Base Score assumes worst case

Temporal score can only go lower than Base Score

CVSS

Metrics

Groups

- Base
- Temporal
- Environmental

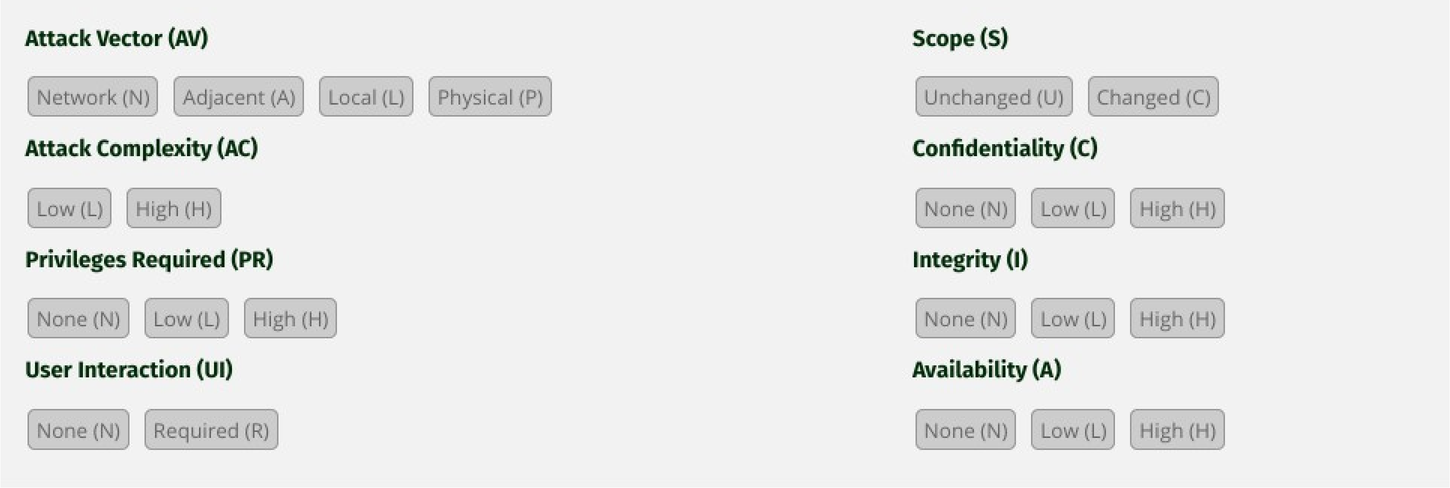
Environmental

- Adjusted to specific environment / org
- Considers mitigating factors
- Considers adverse effect

Can be higher or lower than the Base Score

CVSS

Base Score. Metrics

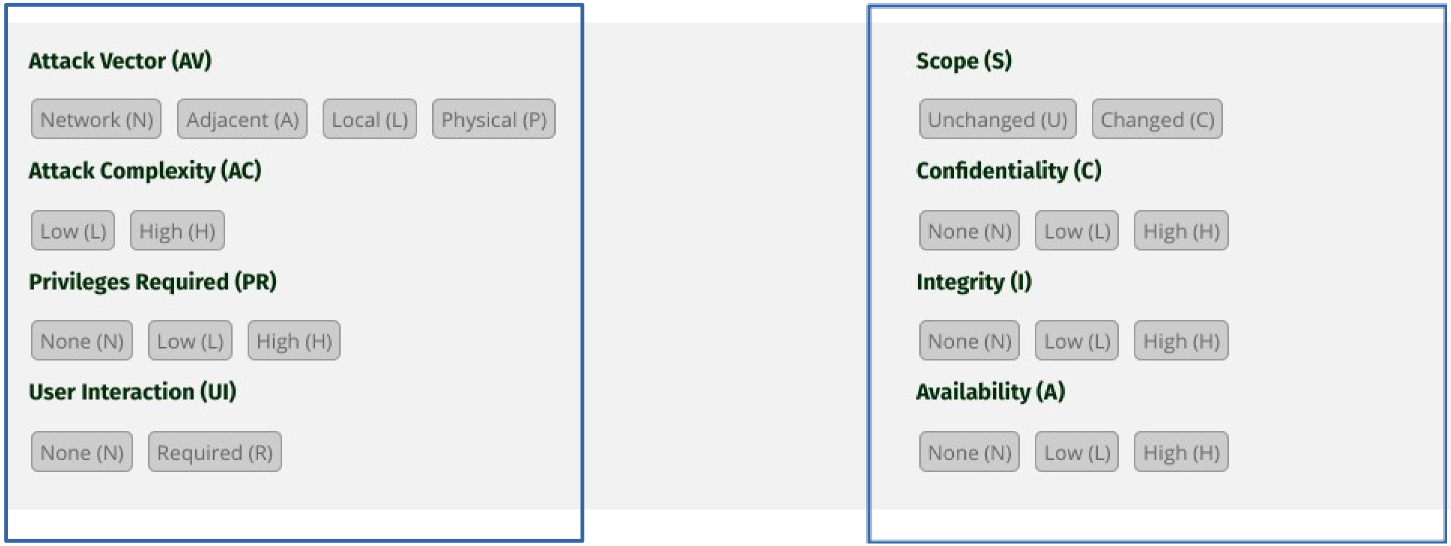


CVSS

Base Score. Metrics

Exploitability

Impact



Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

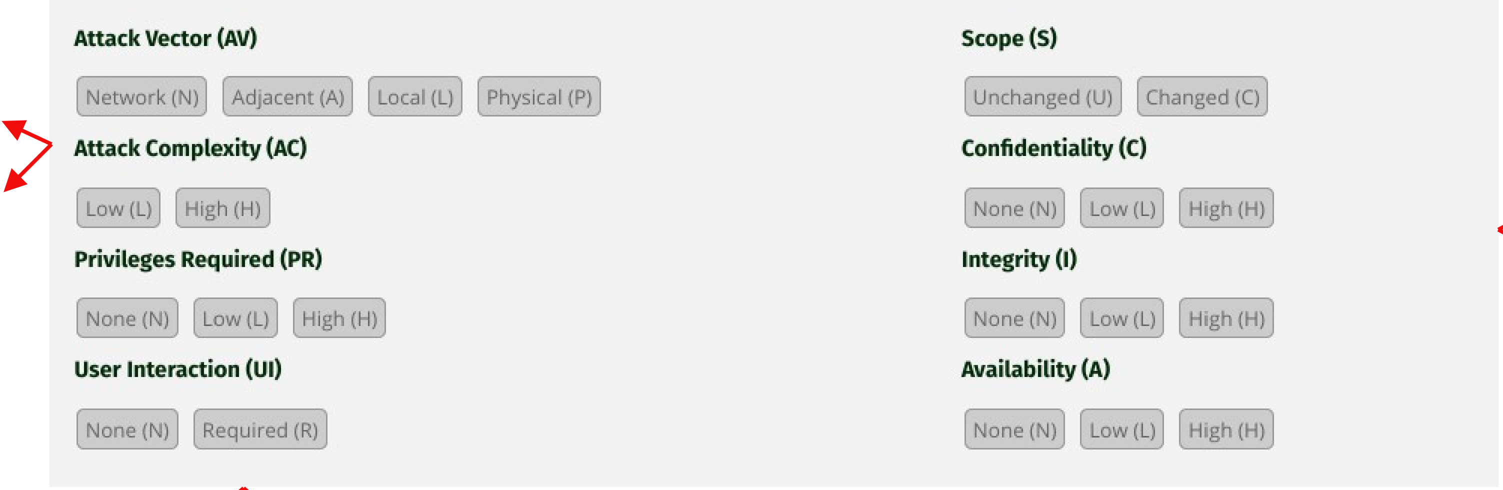
None (N) Low (L) High (H)

Easy → Hard

Small → Big

CVSS

CVSSv3.1 vs CVSSv4.0



Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

Attack Complexity (AC)

Attack Requirements (AT)

Vulnerable (V*)

Subsequent (S*)

Passive (P)

Active (A)

Base Metrics

Attack Vector (AV)

From where can an attacker execute the attack?

Attack Vector (AV)

From where can an attacker execute the attack?

- Network (N)
- Adjacent (A)
- Local (L)
- Physical (P)

Attack Vector (AV)

From where can an attacker execute the attack?

- Network (N)
- Adjacent (A)
- Local (L)
- Physical (P)

Network (N)

Remotely over the network

Examples:

- Web-based attacks

Attack Vector (AV)

From where can an attacker execute the attack?

- Network (N)
- Adjacent (A)
- Local (L)
- Physical (P)

Adjacent (A)

Local/adjacent network (physical or logical)

Examples:

- Physical proximity
  - Bluetooth
  - WiFi
- Logical proximity
  - ARP
  - DHCP

Attack Vector (AV)

From where can an attacker execute the attack?

- Network (N)
- Adjacent (A)
- Local (L)
- Physical (P)

Local (L)

Not bound to the network stack

Examples:

- Vulnerable Lock screen
- Malware infected document
- Local Privilege Escalation (LPE)

Attack Vector (AV)

From where can an attacker execute the attack?

- Network (N)
- Adjacent (A)
- Local (L)
- Physical (P)

Physical (P)

Physical access to the device

Examples:

- Evil Maid
- Infected USB device

Attack Complexity (AT)

Additional requirements (possibly) beyond attacker’s control?

Note: This is not exploit complexity

Attack Complexity (AT)

Additional requirements (possibly) beyond attacker’s control?

- Low (L)
- High (H)

Attack Complexity (AT)

Additional requirements (possibly) beyond attacker’s control?

- Low (L)
- High (H)

Low (L)

No special conditions. Attacker can exploit at will.

Examples:

- Most Web attacks

Attack Complexity (AT)

Additional requirements (possibly) beyond attacker’s control?

- Low (L)
- High (H)

High (H)

Successful attack cannot be accomplished at will

Conditions:

- Knowledge about the environment (topology, architecture, configuration)
- Prepare environment in specific state
- Injection in the logical path

Examples:

- Tight race condition attacks
- Man-in-the-Middle (MitM)

Attack Complexity (AT)

Additional requirements (possibly) beyond attacker’s control?

Split in CVSSv4.0

- Attack Complexity (AC) (security specific measures)
  - ASLR / DEP
  - secrets
- Attact Requirements (AT)
  - MitM

Privileges Required (PR)

What privileges does an attacker need?

Privileges Required (PR)

What privileges does an attacker need?

- None (N)
- Low (L)
- High (H)

Privileges Required (PR)

What privileges does an attacker need?

- None (N)
- Low (L)
- High (H)

None (N)

No need for authentication

Examples:

- SQL injection on the login page

Privileges Required (PR)

What privileges does an attacker need?

- None (N)
- Low (L)
- High (H)

Low (L)

Authentication required, but only low privileges

Examples:

- Low-privileged user can access the admin panel
- Logged in attacker is able to change other user’s data

Privileges Required (PR)

What privileges does an attacker need?

- None (N)
- Low (L)
- High (H)

High (H)

Attacker needs significant privileges (e.g. admin)

Examples:

- Exploit only possible through the admin panel of a Web app

* Only score what is gained

User Interaction (UI)

Does a user/victim need to do something?

User Interaction (UI)

Does a user/victim need to do something?

- None (N)
- Required (R)

User Interaction (UI)

Does a user/victim need to do something?

- None (N)
- Required (R)

None (N)

Attacker can exploit without any interaction from any user/victim

Examples:

- SQL injection on the login page

User Interaction (UI)

Does a user/victim need to do something?

- None (N)
- Required (R)

Required (R)

Attacker needs to “trick” the victim into doing something or has to wait for them to perform specific operation

Examples:

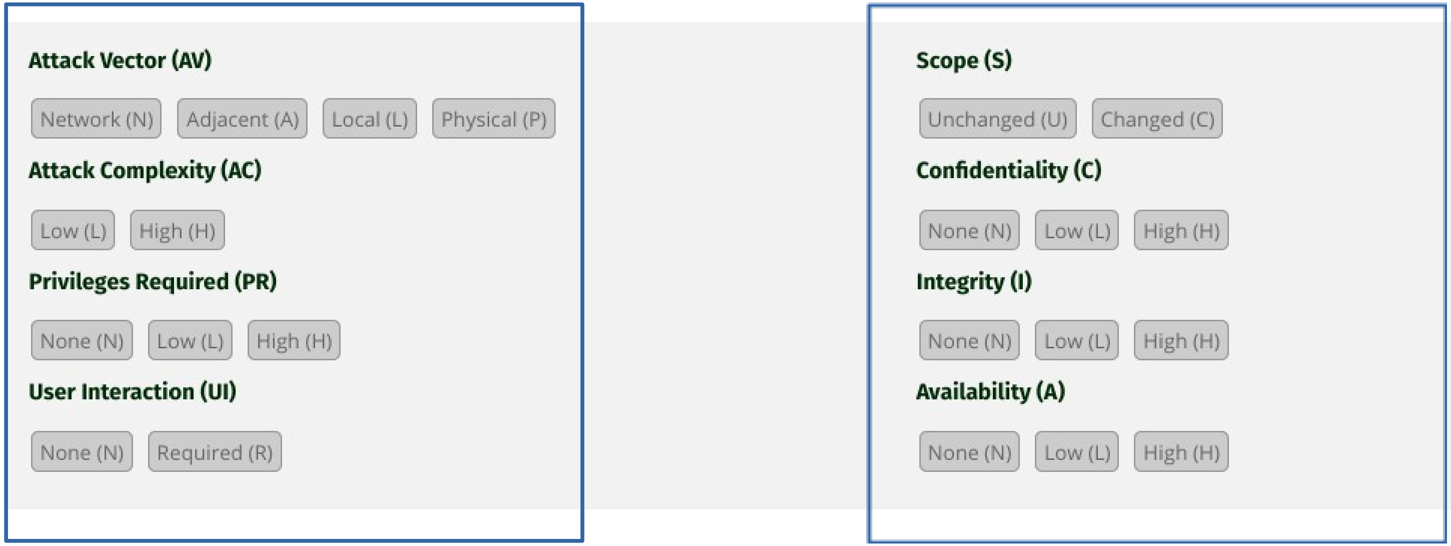
- Cross-Site-Scripting (XSS)
- Malicious email attachment

CVSS

Base Score. Metrics

Exploitability

Impact



Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

None (N) Low (L) High (H)

Easy → Hard

Small → Big

Scope (S)

Does it affect other components beyond the vulnerable component’s security scope / trust boundary?

Scope (S)

Affects components beyond the security scope?

- Unchanged (U)
- Changed (C)

Scope (S)

Affects components beyond the security scope?

- Unchanged (U)
- Changed (C)

Unchanged (U)

Vulnerable component and impacted component are the same

Examples:

- User enumeration
- Authentication bypass

Scope (S)

Affects components beyond the security scope?

- Unchanged (U)
- Changed (C)

Changed (C)

Vulnerable component and impacted component are different and managed by different security authorities

Examples:

- Container escape
- VM escape
- Reflected Cross-Site-Scripting (XSS)

CIA

Confidentiality

Integrity

Availability

Security Properties

CIA

- Confidentiality
- Integrity
- Availability

Security Properties

CIA

- Confidentiality
- Integrity
- Availability

Confidentiality

Attackers can’t read the data

Security Properties

CIA

- Confidentiality
- Integrity
- Availability

Integrity

Attackers can’t modify the data

Security Properties

CIA

- Confidentiality
- Integrity
- Availability

Availability

Attackers can’t disrupt the service

CIA Impacts

Confidentiality Integrity Availability

• None (N)	Only what is gained
• Low (L)	Only what is proven (reasonably expected)
• High (H)	

CIA Impacts

Confidentiality Integrity Availability

- None (N)
- Low (L)
- High (H)

None (N)

No impact

Confidentiality

No loss

Integrity

No loss

Availability

No loss

CIA Impacts

Confidentiality Integrity Availability

- None (N)
- Low (L)
- High (H)

Low (L)

Some impact

Confidentiality

Access to some restricted data

- No control over which data
- Amount/kind is limited

Integrity

Only some data can be modified

- No control over which data
- Amount/kind is limited

Availability

Some impact (e.g. performance) or partial impact. Attacker can’t completely deny service

CIA Impacts

Confidentiality Integrity Availability

- None (N)
- Low (L)
- High (H)

High (H)

Major or full impact

Confidentiality

All data or critical data

Integrity

All data or critical data

Availability

Fully deny access

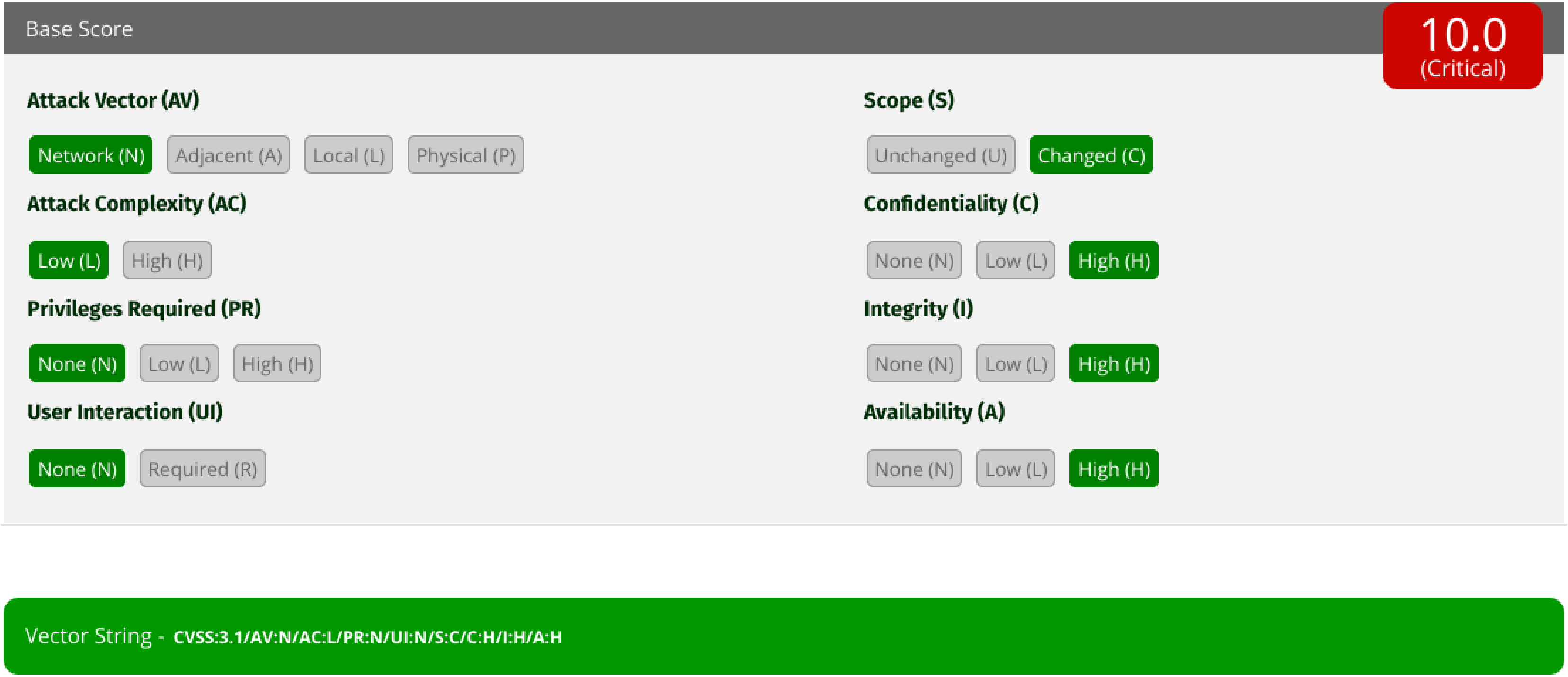
- Sustained (during attack)
- Persistent (even after attack)

Deny only access to some critical resource

- Log, new connections/sessions

CVSS

Score and Vector



Base Score

10.0
(Critical)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

Unchanged (U) [✓ Changed (C)]

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

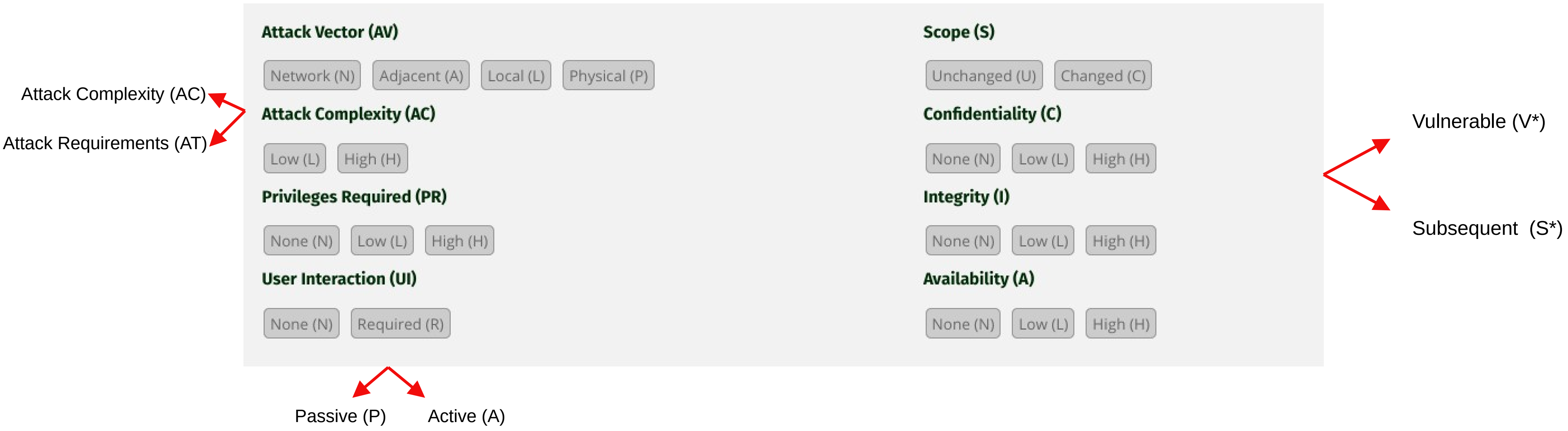
Availability (A)

None (N) Low (L) [✓ High (H)]

Vector String - **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H**

CVSS

CVSSv3.1 vs CVSSv4.0



Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

None (N) Low (L) High (H)

Attack Complexity (AC)

Attack Requirements (AT)

Vulnerable (V*)

Subsequent (S*)

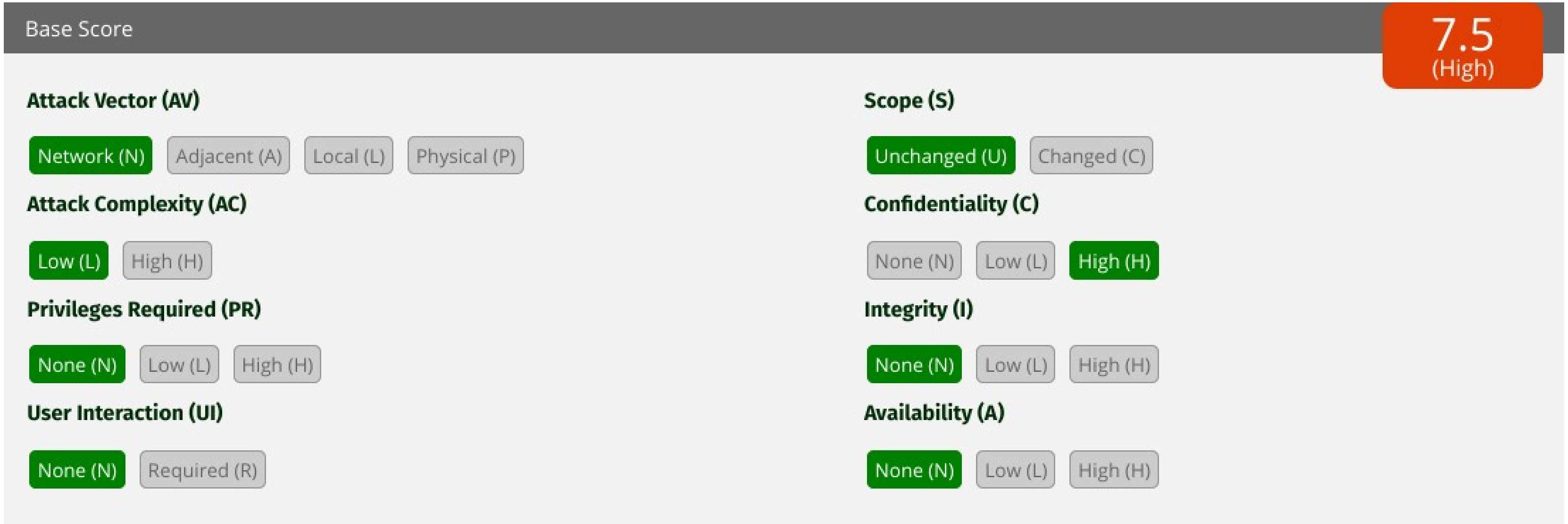
Passive (P)

Active (A)

Examples

CVE-2025-4427

An authentication bypass in the API component of Ivanti Endpoint Manager Mobile 12.5.0.0 and prior allows attackers to access protected resources without proper credentials via the API.



Base Score

7.5 (High)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

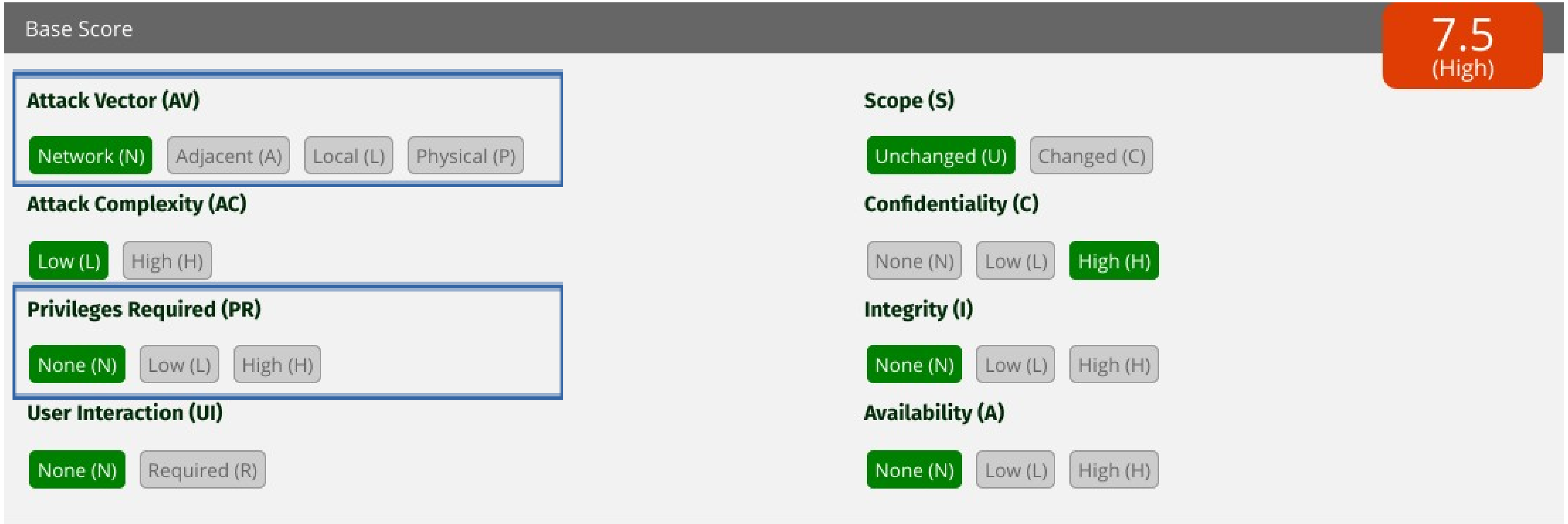
[✓ None (N)] Low (L) High (H)

Availability (A)

[✓ None (N)] Low (L) High (H)

CVE-2025-4427

An authentication bypass in the API component of Ivanti Endpoint Manager Mobile 12.5.0.0 and prior allows attackers to access protected resources without proper credentials via the API.



Base Score

7.5 (High)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

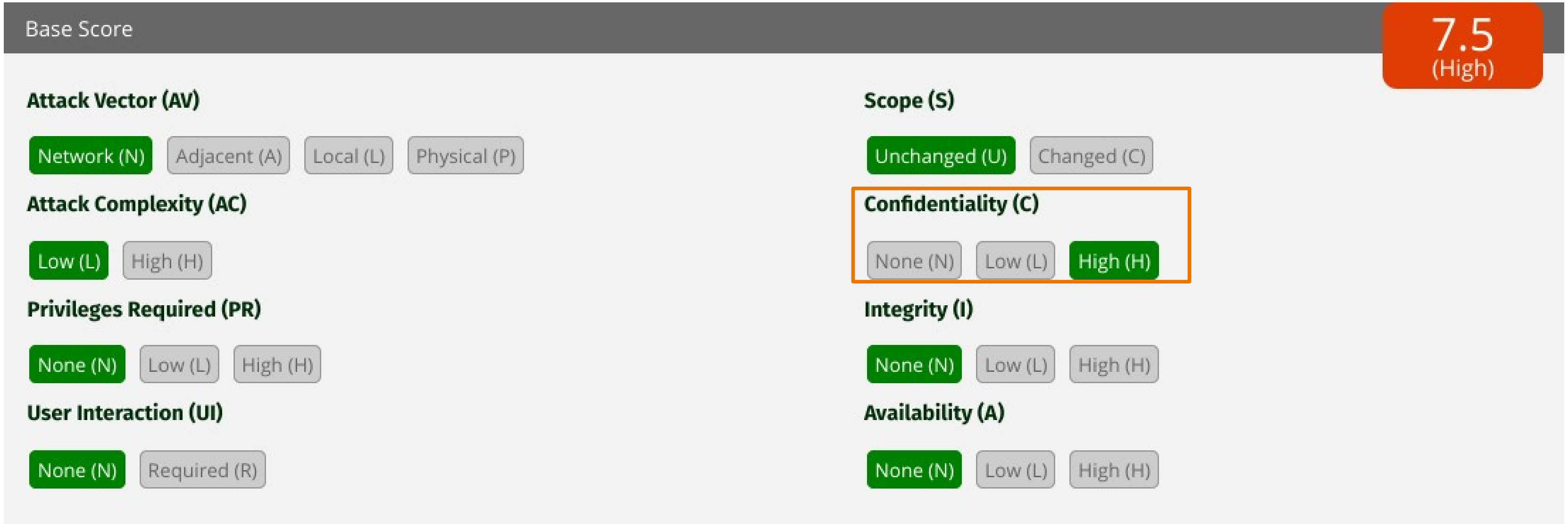
[✓ None (N)] Low (L) High (H)

Availability (A)

[✓ None (N)] Low (L) High (H)

CVE-2025-4427

An authentication bypass in the API component of Ivanti Endpoint Manager Mobile 12.5.0.0 and prior allows attackers to access protected resources without proper credentials via the API.



Base Score

7.5
(High)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

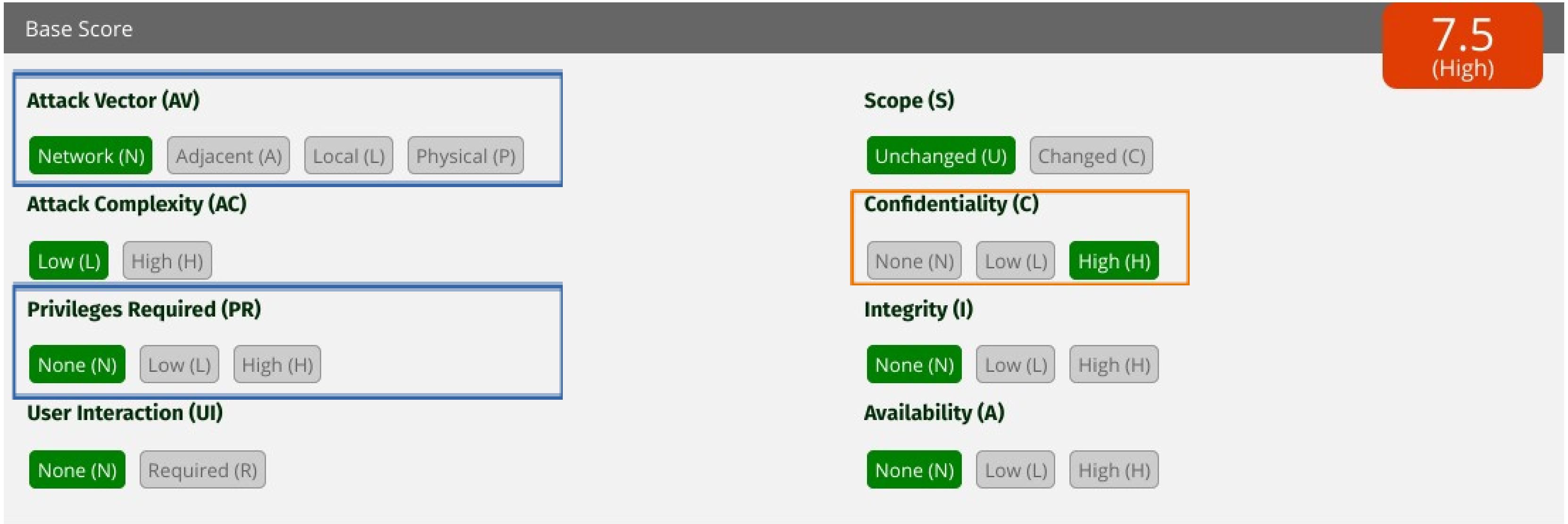
[✓ None (N)] Low (L) High (H)

Availability (A)

[✓ None (N)] Low (L) High (H)

CVE-2025-4427

An authentication bypass in the API component of Ivanti Endpoint Manager Mobile 12.5.0.0 and prior allows attackers to access protected resources without proper credentials via the API.



Base Score

7.5
(High)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

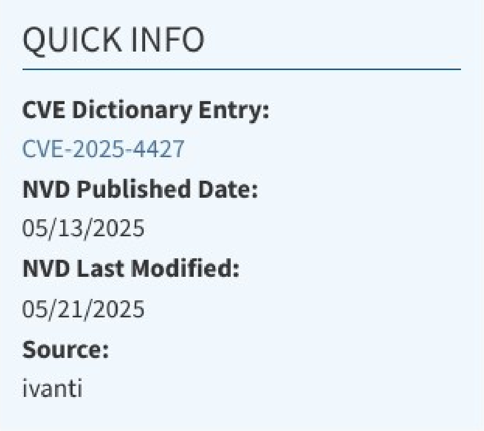
[✓ None (N)] Low (L) High (H)

Availability (A)

[✓ None (N)] Low (L) High (H)

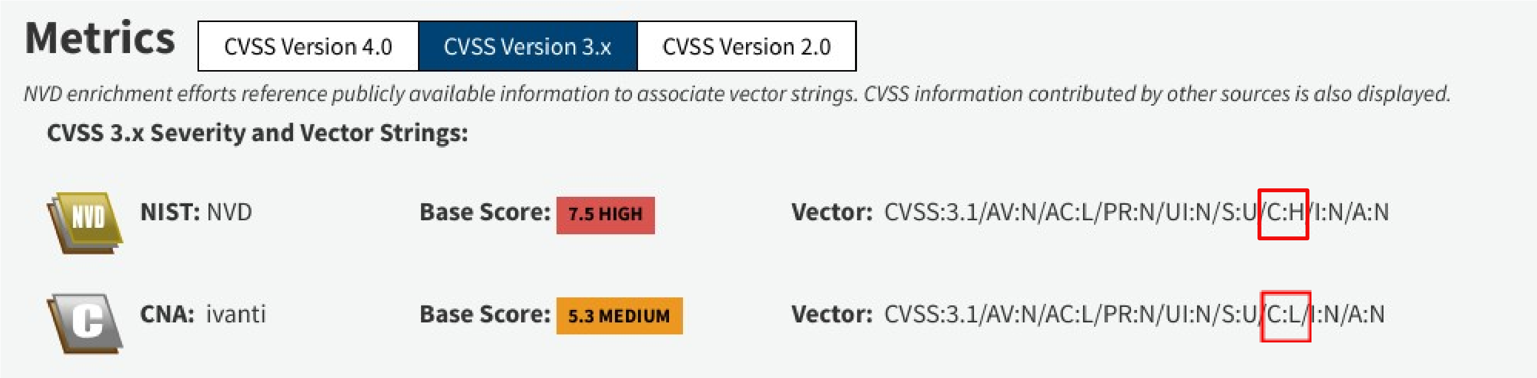
CVSS

CVE-2025-4427



QUICK INFO

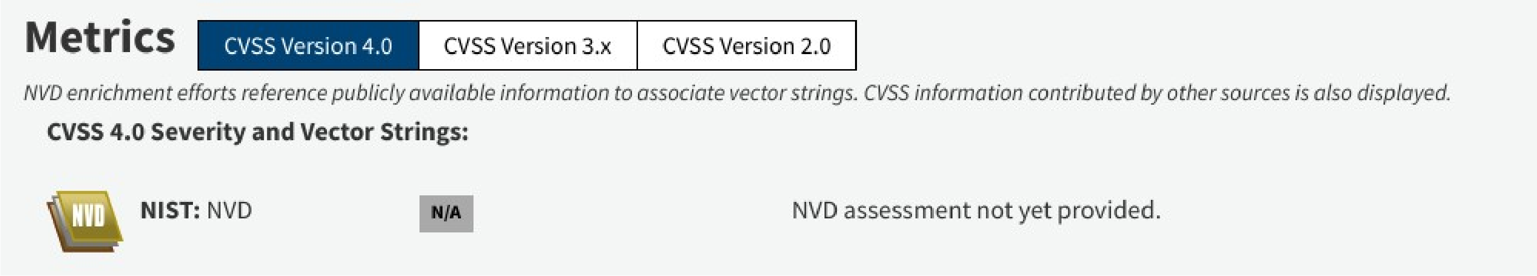
CVE Dictionary Entry:
CVE-2025-4427
NVD Published Date:
05/13/2025
NVD Last Modified:
05/21/2025
Source:
ivanti



NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD	**Base Score:** 7.5 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CNA: ivanti	**Base Score:** 5.3 MEDIUM	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N



NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

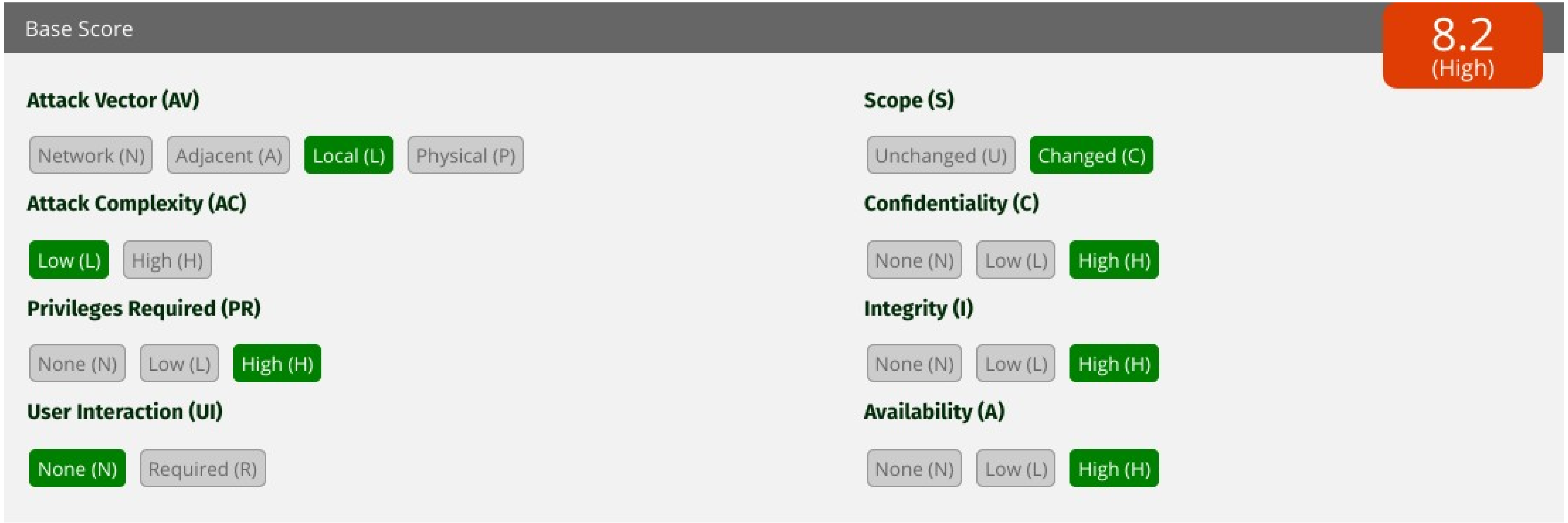
CVSS 4.0 Severity and Vector Strings:

NIST: NVD	N/A	NVD assessment not yet provided.

https://nvd.nist.gov/vuln/detail/cve-2025-4427

CVE-2020-4004

VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG), Workstation (15.x before 15.5.7), Fusion (11.x before 11.5.7) contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.



Base Score

8.2
(High)

Attack Vector (AV)
Local (L)

Attack Complexity (AC)
Low (L)

Privileges Required (PR)
High (H)

User Interaction (UI)
None (N)

Scope (S)
Changed (C)

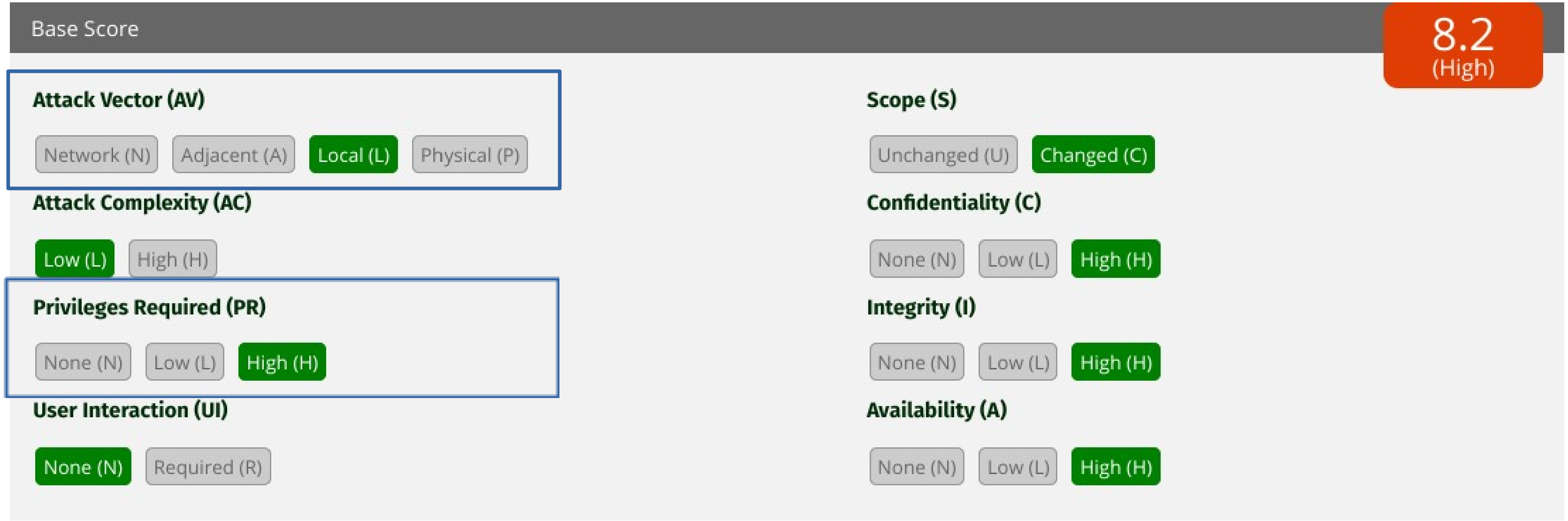
Confidentiality (C)
High (H)

Integrity (I)
High (H)

Availability (A)
High (H)

CVE-2020-4004

VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG), Workstation (15.x before 15.5.7), Fusion (11.x before 11.5.7) contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.



Base Score

8.2 (High)

Attack Vector (AV)

Network (N) Adjacent (A) [✓ Local (L)] Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

None (N) Low (L) [✓ High (H)]

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

Unchanged (U) [✓ Changed (C)]

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

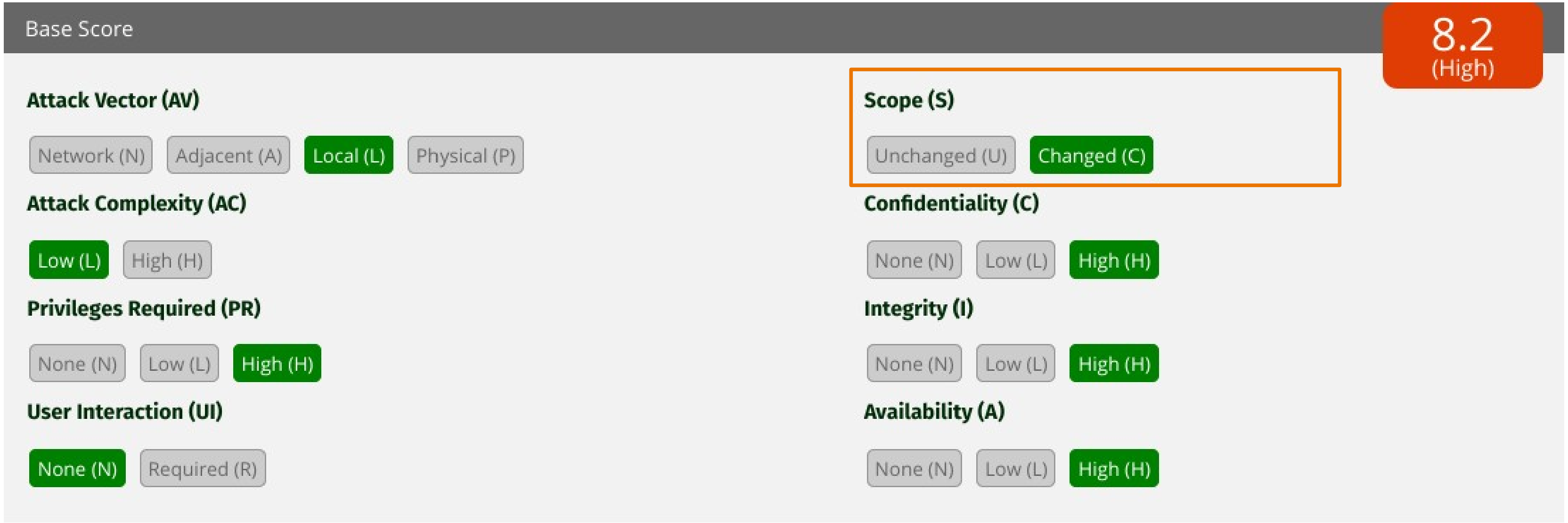
None (N) Low (L) [✓ High (H)]

Availability (A)

None (N) Low (L) [✓ High (H)]

CVE-2020-4004

VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG), Workstation (15.x before 15.5.7), Fusion (11.x before 11.5.7) contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.



Base Score

8.2
(High)

Attack Vector (AV)

Network (N) Adjacent (A) [✓ Local (L)] Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

None (N) Low (L) [✓ High (H)]

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

Unchanged (U) [✓ Changed (C)]

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

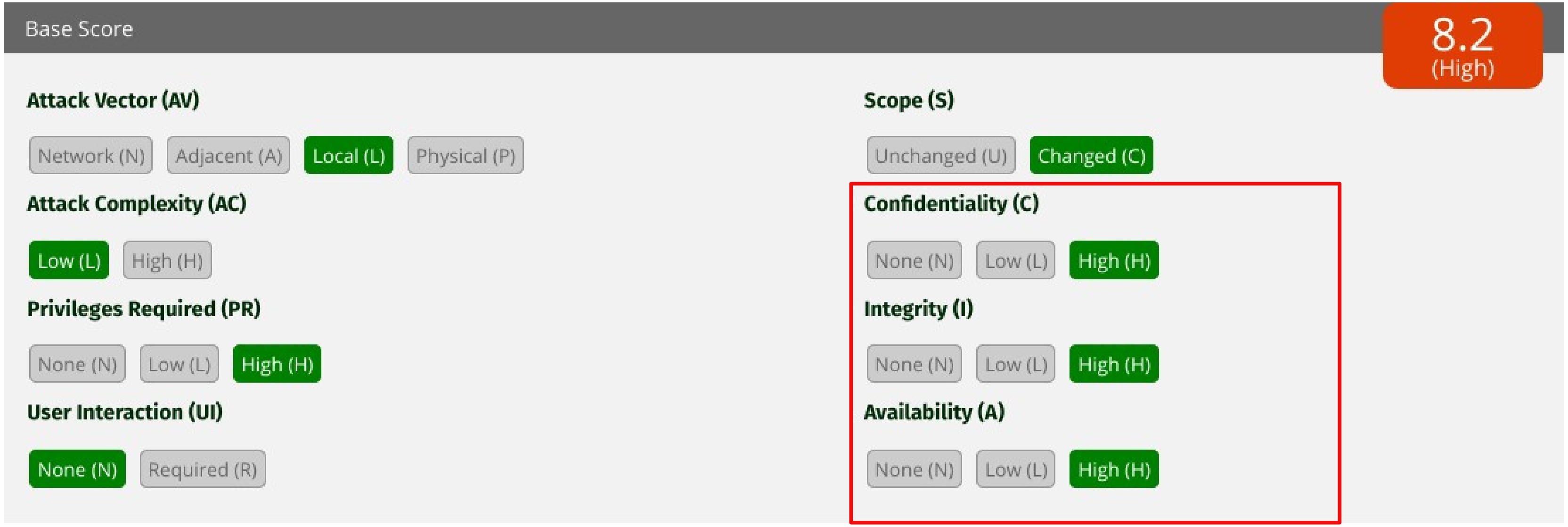
None (N) Low (L) [✓ High (H)]

Availability (A)

None (N) Low (L) [✓ High (H)]

CVE-2020-4004

VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG), Workstation (15.x before 15.5.7), Fusion (11.x before 11.5.7) contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.



Base Score

8.2
(High)

Attack Vector (AV)

Network (N) Adjacent (A) [✓ Local (L)] Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

None (N) Low (L) [✓ High (H)]

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

Unchanged (U) [✓ Changed (C)]

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

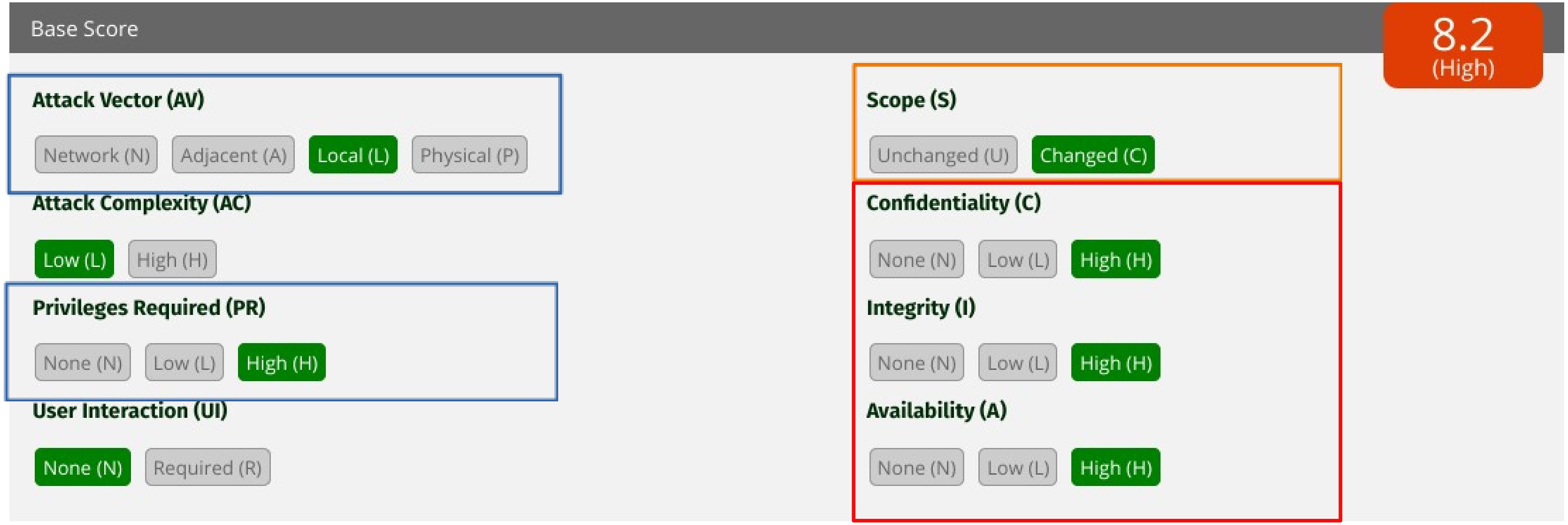
None (N) Low (L) [✓ High (H)]

Availability (A)

None (N) Low (L) [✓ High (H)]

CVE-2020-4004

VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG), Workstation (15.x before 15.5.7), Fusion (11.x before 11.5.7) contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.



Base Score

8.2
(High)

Attack Vector (AV)

Network (N) Adjacent (A) [✓ Local (L)] Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

None (N) Low (L) [✓ High (H)]

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

Unchanged (U) [✓ Changed (C)]

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

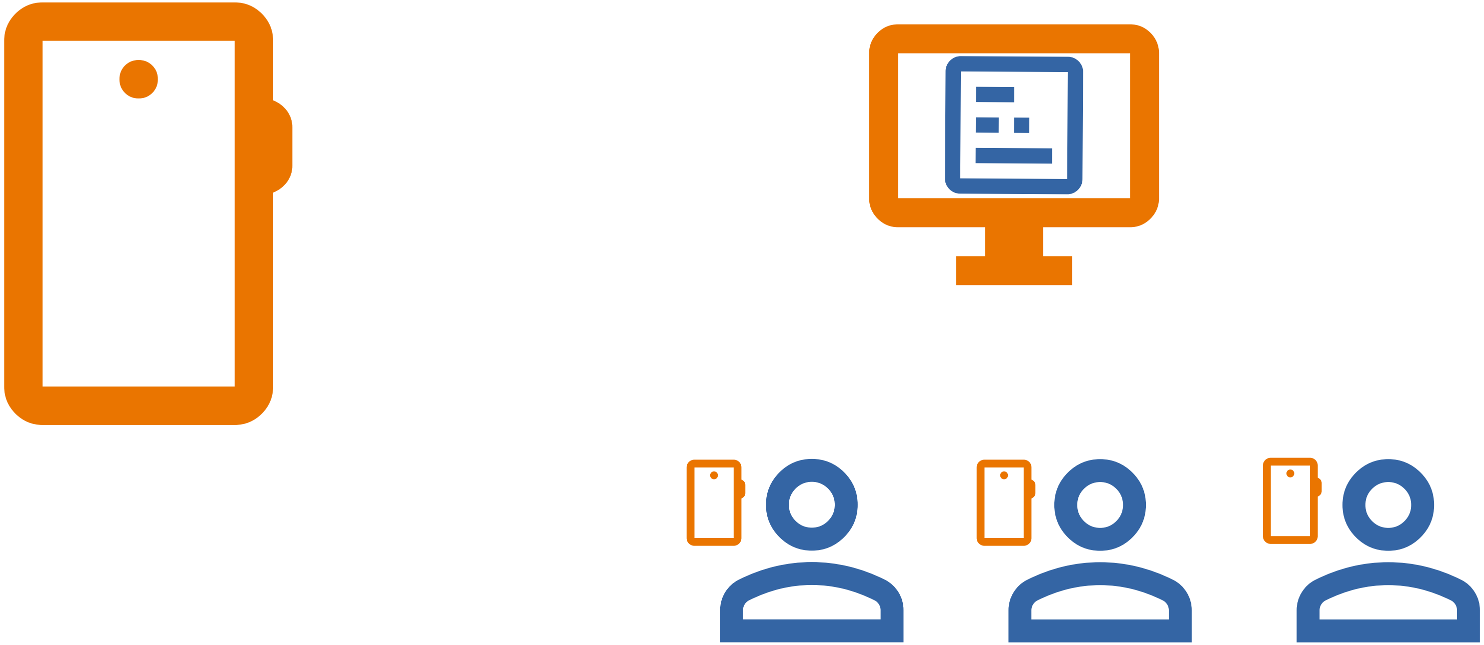
None (N) Low (L) [✓ High (H)]

Availability (A)

None (N) Low (L) [✓ High (H)]

CVSS Scoring

Live Session



You are about to visit:

fit-turtle-nice.ngrok-free.app

Website IP:

- This website is served for free through ngrok.com.
- You should only visit this website if you trust whoever sent the link to you.
- Be careful about disclosing personal or financial information like passwords, phone numbers, or credit cards.

Visit Site

Example 1

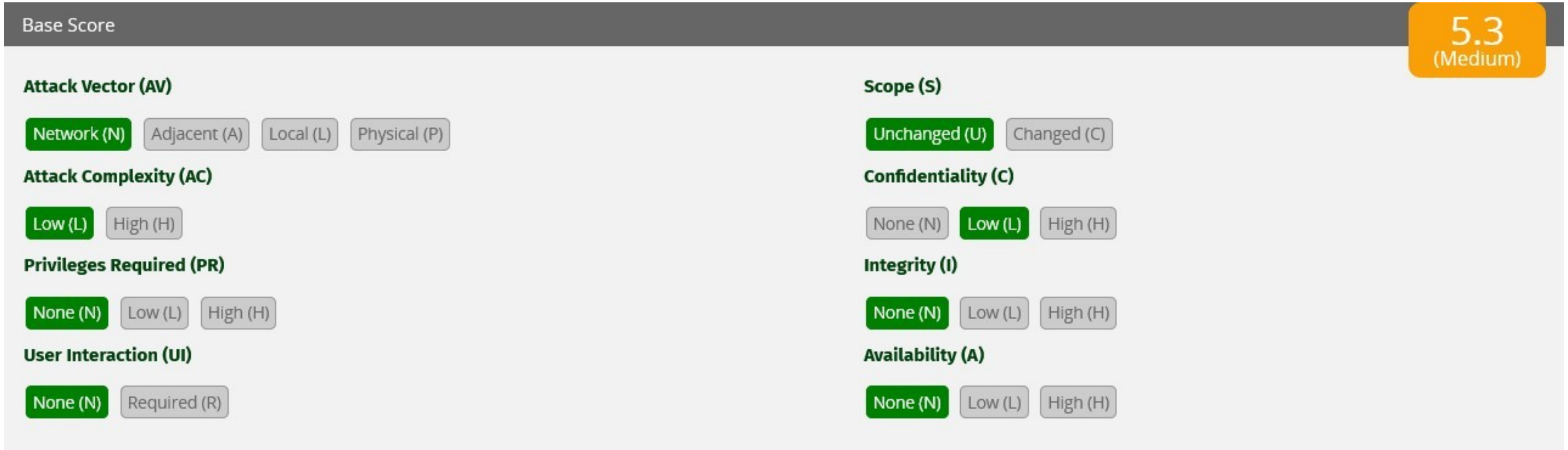
SaaS

Unauthenticated attacker can list registered users of a SaaS offering

Example 1

SaaS

Unauthenticated attacker can list registered users of a SaaS offering



Base Score

5.3
(Medium)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) [✓ Low (L)] High (H)

Integrity (I)

[✓ None (N)] Low (L) High (H)

Availability (A)

[✓ None (N)] Low (L) High (H)

Example 2

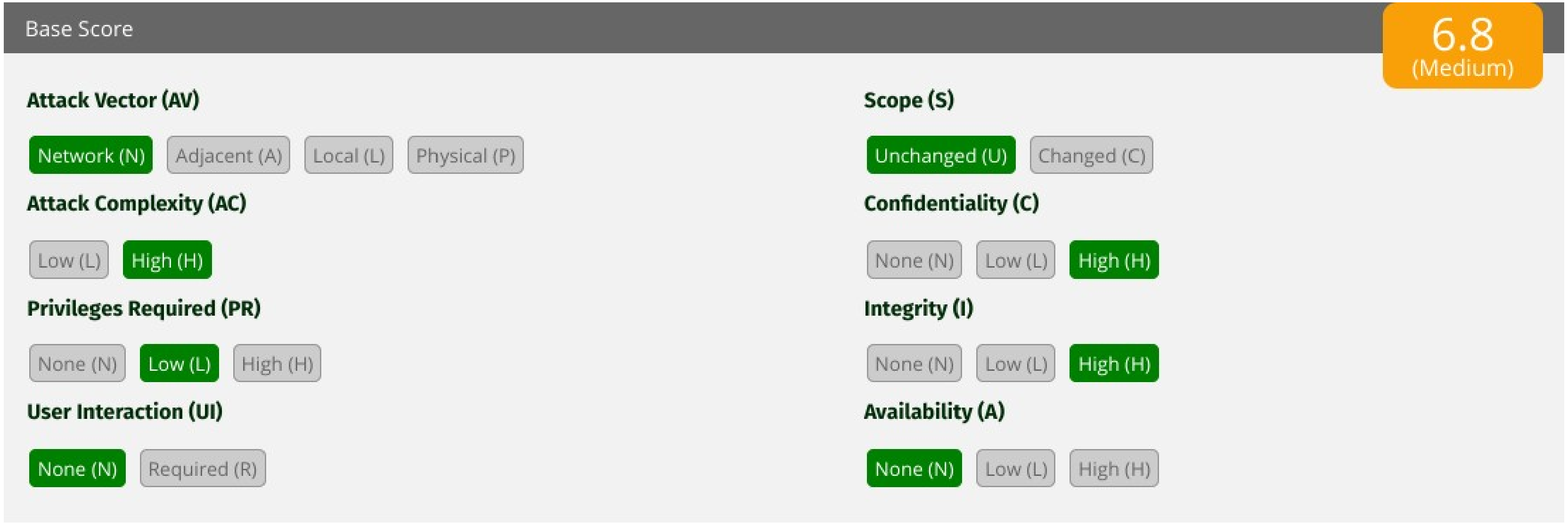
SaaS. IDOR

A malicious SaaS user with knowledge of another user’s 80-bit unique userid, can arbitralily set their password.

Example 2

SaaS. IDOR

A malicious SaaS user with knowledge of another user’s 80-bit unique userid, can arbitralily set their password.



Base Score

6.8 (Medium)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) [✓ High (H)]

Privileges Required (PR)

None (N) [✓ Low (L)] High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

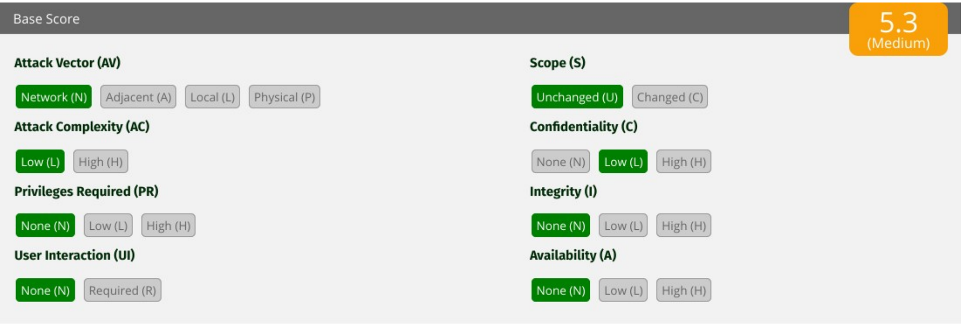
Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

[✓ None (N)] Low (L) High (H)

Chaining Vulnerabilities



Base Score 5.3 (Medium)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

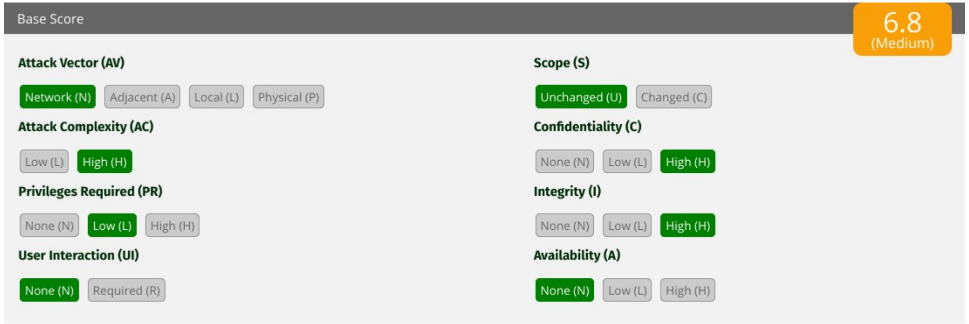
None (N) [✓ Low (L)] High (H)

Integrity (I)

[✓ None (N)] Low (L) High (H)

Availability (A)

[✓ None (N)] Low (L) High (H)



Base Score 6.8 (Medium)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) [✓ High (H)]

Privileges Required (PR)

None (N) [✓ Low (L)] High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

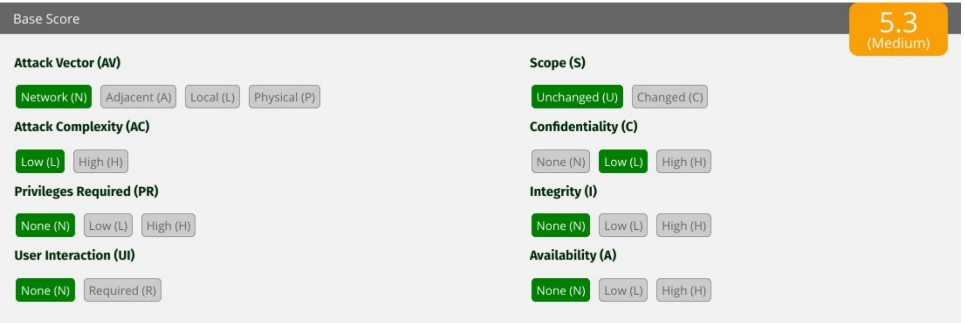
Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

[✓ None (N)] Low (L) High (H)

Chaining Vulnerabilities



Base Score

5.3 (Medium)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

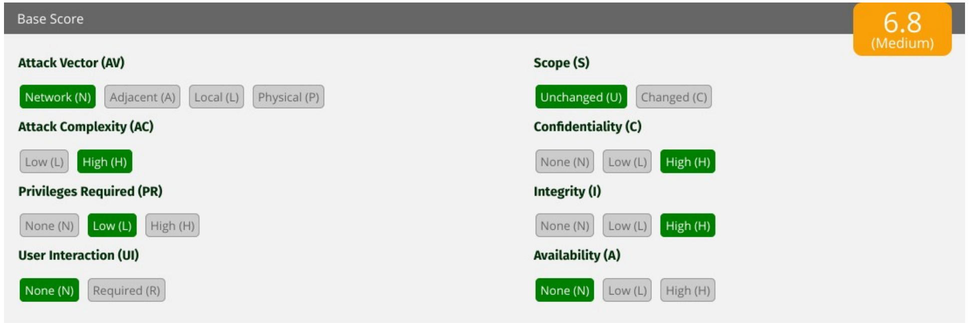
None (N) [✓ Low (L)] High (H)

Integrity (I)

[✓ None (N)] Low (L) High (H)

Availability (A)

[✓ None (N)] Low (L) High (H)



Base Score

6.8 (Medium)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) [✓ High (H)]

Privileges Required (PR)

None (N) [✓ Low (L)] High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

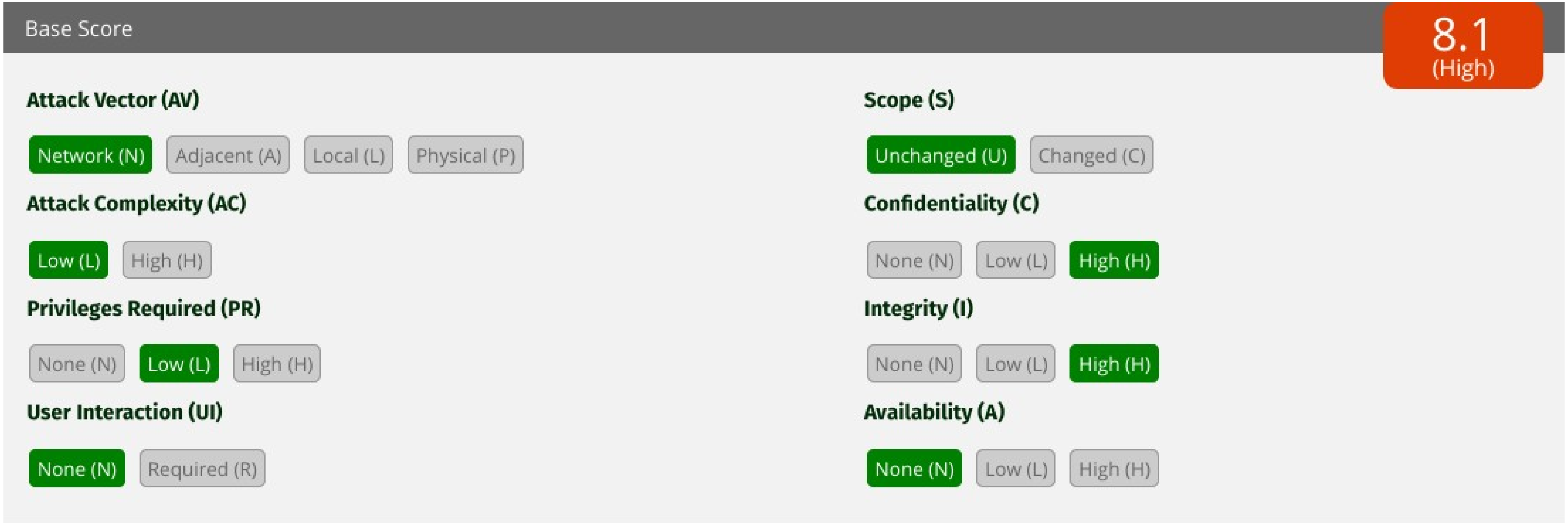
None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

[✓ None (N)] Low (L) High (H)



Base Score

8.1 (High)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

None (N) [✓ Low (L)] High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

[✓ None (N)] Low (L) High (H)

Example 3

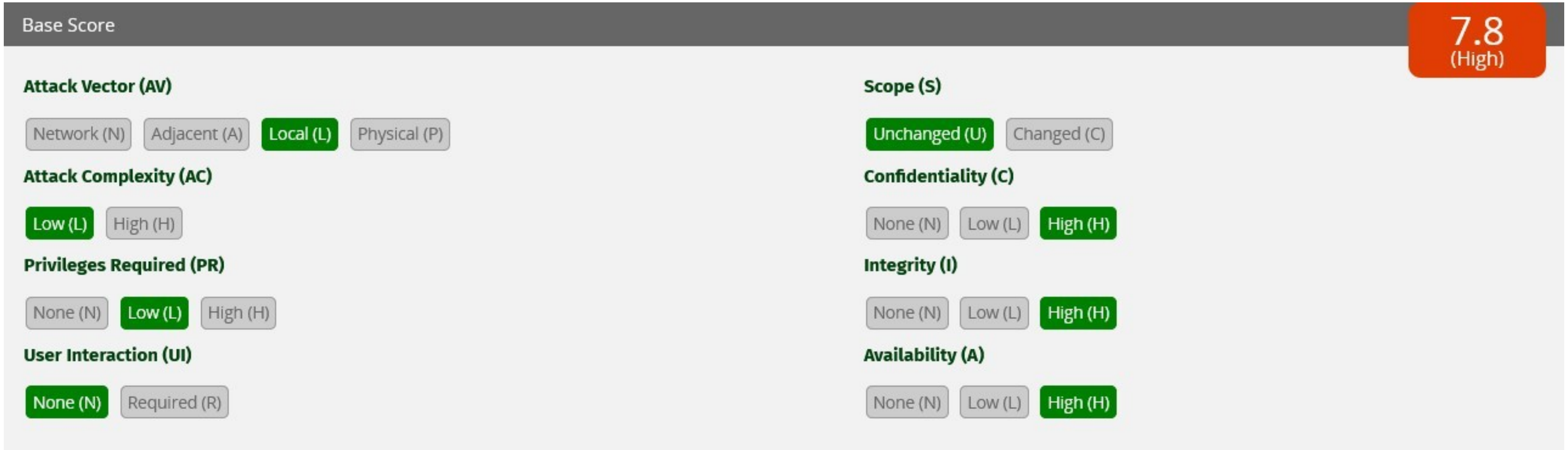
Linux Kernel Vulnerability

In the Linux kernel through 6.3.1, a use-after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled.

Example 3

Linux Kernel Vulnerability. CVE-2023-32233

In the Linux kernel through 6.3.1, a use-after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled.



Base Score

7.8
(High)

Attack Vector (AV)

Network (N) Adjacent (A) [✓ Local (L)] Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

None (N) [✓ Low (L)] High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

None (N) Low (L) [✓ High (H)]