PS-CVSS

Physical Security Scoring Reference | v1.1

LOW	MEDIUM	HIGH	CRITICAL
1.0–1.6	1.7–2.4	2.5–3.2	3.3–4.0

Score each finding across 6 metrics (1–4 pts each). Sum and divide by 6.

+1 LOW +2 MEDIUM +3 HIGH +4 CRITICAL

AV	**Access Vector** Where does the attacker start?	+1	**(P) Perimeter** Must breach fencing, gates, or outer barriers before reaching the building.	**SC**	**Scope of Compromise** What access is gained if exploited?	+1	**(L) Limited** One room or small contained area. Impact is local and isolated.
		+2	**(E) Exterior** Attack possible from the building exterior or publicly accessible grounds.			+2	**(Z) Zone** Extends to a floor, wing, or defined security zone within the facility.
		+3	**(I) Interior** Attacker is already inside the facility. No perimeter or exterior breach needed.			+3	**(F) Facility** Full facility access achievable. All areas reachable from this entry point.
		+4	**(U) Unrestricted** No barrier exists. The target is openly reachable by anyone.			+4	**(M) Multi-site** Access across multiple sites or systemic shared infrastructure.
AC	**Access Complexity** How much effort does exploitation require?	+1	**(H) High** Specialized tools or advanced skill required. Not an opportunistic attack.	**CI**	**Consequence Impact** What is the worst-case outcome?	+1	**(I) Info** Low-sensitivity information or non-critical area. Easily contained.
		+2	**(M) Medium** Basic preparation or common tools needed. Achievable with modest effort.			+2	**(D) Disruption** Operations disrupted, equipment tampered, or staff safety put at risk.
		+3	**(L) Low** Minimal skill, no special tools. Most attackers can execute this reliably.			+3	**(C) Compromise** Sensitive data, credentials, or critical IT systems accessed or exfiltrated.
		+4	**(N) None** Zero effort. Anyone can exploit this with no preparation or tools whatsoever.			+4	**(X) Catastrophic** Physical harm to personnel or irreversible facility damage is possible.
DL	**Detection Likelihood** How likely is the attacker to be detected?	+1	**(H) High** Active monitoring. Cameras, guards, or staff would likely detect and respond.	**SE**	**SE Required** Was social engineering needed to exploit this?	+1	**(C) Complex** Elaborate pretext, props, or a multi-step deception campaign required.
		+2	**(M) Medium** Some monitoring exists but gaps allow execution without guaranteed detection.			+2	**(A) Active** Must engage, build rapport, and actively deceive one or more employees.
		+3	**(L) Low** Monitoring is sparse or inactive. Low risk of being seen during execution.			+3	**(P) Passive** Attacker only needs to blend in. No conversation or active deception required.
		+4	**(N) None** No effective detection. Attacker can operate freely without realistic risk of notice.			+4	**(N) None** No social engineering required. Purely physical or technical vulnerability.

Score = (AV + AC + DL + SC + CI + SE) / 6

FORMAT	`AV:[v] / AC:[v] / DL:[v] / SC:[v] / CI:[v] / SE:[v] = [score] ([severity])`
EXAMPLE	`AV:E / AC:N / DL:L / SC:F / CI:C / SE:N = 3.2 (HIGH)`

SCORING WORKSHEET

METRIC	ID	QUICK REFERENCE	METRIC	ID	QUICK REFERENCE
Access Vector	**AV**	P=1 E=2 I=3 U=4	Scope of Compromise	**SC**	L=1 Z=2 F=3 M=4
Access Complexity	**AC**	H=1 M=2 L=3 N=4	Consequence Impact	**CI**	I=1 D=2 C=3 X=4
Detection Likelihood	**DL**	H=1 M=2 L=3 N=4	SE Required	**SE**	C=1 A=2 P=3 N=4
RAW TOTAL					
DIVIDED BY 6					
PS-CVSS SCORE		1.0–1.6 LOW / 1.7–2.4 MED / 2.5–3.2 HIGH / 3.3–4.0 CRIT			

NOTE When multiple assessors score the same finding, review any metric where scores differ by more than one point before finalizing. The goal is defensible, repeatable scoring across the engagement.

SCORED EXAMPLES

Server room unsecured during after-hours access window

CRITICAL 3.8

Server room door propped open and unattended during a scheduled after-hours maintenance window. No access log recorded, no camera on interior.

`AV:I / AC:N / DL:N / SC:M / CI:X / SE:N`

SC:M because server room access impacts all connected systems organization-wide. SE:N + AC:N + DL:N + CI:X all at maximum.

Wiegand readers, credentials in cleartext

HIGH 3.0

HID proximity readers on all exterior doors use Wiegand protocol. Credentials transmitted without encryption. Susceptible to passive interception.

`AV:E / AC:M / DL:N / SC:F / CI:C / SE:N`

SE:N (+4) means no human barrier existed. DL:N + SC:F push this to 3.0 HIGH. Systemic finding across every exterior door with no detection.

Fire exit door propped open, no alarm triggered

HIGH 3.2

East side fire exit found propped with a door wedge. Door position sensor non-functional. No alarm triggered, no staff response observed.

`AV:E / AC:N / DL:L / SC:F / CI:C / SE:N`

SE:N (+4) and AC:N (+4) mean zero effort, no human element. DL:L keeps it HIGH rather than CRITICAL. Some monitoring exists but did not trigger.

IT vendor pretext, access to wiring closet

MEDIUM 2.0

Assessor posing as an IT vendor gained access to a wiring closet. Staff escorted without verifying identity or work order.

`AV:E / AC:M / DL:M / SC:Z / CI:D / SE:A`

SE:A (+2) shows physical controls forced active deception. Swap SE:A for SE:N and this jumps to 2.7 HIGH. The SE value alone changes the severity.

Sensitive documents on unattended workstations

MEDIUM 1.8

Documents labeled Internal visible on multiple unattended desks. No clean desk enforcement observed.

`AV:I / AC:L / DL:M / SC:L / CI:I / SE:C`

SE:C (+1) reflects strong physical controls. An elaborate pretext would be needed. CI:I and SC:L cap the score at MEDIUM regardless of other metrics.

Visitor log left visible at unattended reception desk

LOW 1.5

Visitor log with names, companies, and host employees left open on an unattended reception desk.

`AV:E / AC:L / DL:H / SC:L / CI:I / SE:C`

DL:H (+1) keeps the score low. Active monitoring at reception limits risk. SE:C (+1) reflects that further exploitation would require a sophisticated pretext.

PS-CVSS: proprietary framework by redteam.vip for authorized physical security assessments. Not affiliated with FIRST or the official CVSS standard. Scores are advisory. | v1.1