

Rule Report — rule-20120ee2

Created: 2025-10-03T08:27:57Z | Threat Level: Critical

Executive summary: Detected OS_FINGERPRINT from 172.20.10.4 targeting N/A.

Technical summary

Field	Value
Rule ID	rule-20120ee2
Alert Type	OS_FINGERPRINT
Src IP	172.20.10.4
Target IP	N/A
Ports	N/A
CVSS	9.8
Risk score	89.0 (Critical)
Decision	notify — OS Fingerprinting detected

Correlation / Related alerts

Related alerts (last 48h): **128**



Enrichment

Country	N/A
City	N/A
Reputation Score	0.5
IP Info Raw	None

Evidence

Raw alert: `{"alert_type": "OS FINGERPRINT", "src_ip": "172.20.10.4", "target_ip": null, "ports": [], "start_time": "Wed Jul 30 15:25:23 2025", "duration": null}`

Capture Time: Wed Jul 30 15:25:23 2025