Vulnerability Scan Report - OpenVAS Export

Classification: SAMPLE | Fictional demonstration data | Exported from OpenVAS (Greenbone)

Scan summary

Target: 10.0.0.5 (example host) Scan: Full and fast 2026-08-20 09:00 UTC

Results: 1 High | 3 Medium | 6 Low | 21 Log

HIGH - Apache 2.4.49 path traversal (CVE-2021-41773)

Affected: example-web-01 (10.0.0.5:443)

MEDIUM - SSH allows weak key-exchange algorithms

MEDIUM - Self-signed TLS certificate on management interface

MEDIUM - SMB signing not required

LOW - Outdated OpenSSH banner (information disclosure)

LOW - ICMP timestamp requests enabled