

Network Scan Report

Device: 192.168.1.1

Service	Version
Dropbear sshd	unknown

Device: 192.168.1.223

Service	Version
AirTunes rtspd	377.40.00

Device: 192.168.1.132

Device: 192.168.1.239

Service	Version
VMware Authentication Daemon	1.10
VMware Authentication Daemon	1.0
Microsoft HTTPAPI httpd	2.0

Device: 192.168.1.143

Service	Version
Apache httpd	2.4.23
Microsoft Windows RPC	unknown
Microsoft Windows netbios-ssn	unknown
Microsoft Windows 7 - 10 microsoft-ds	unknown
Microsoft HTTPAPI httpd	2.0
Microsoft Windows RPC	unknown

Microsoft Windows RPC	unknown
Microsoft Windows RPC	unknown
Microsoft Windows RPC	unknown
Microsoft Windows RPC	unknown
Microsoft Windows RPC	unknown

Vulnerabilities & Risk Scoring

Apache httpd 2.4.23 — Risk Score: 100

- CVE-2017-3167 (HIGH): Authentication bypass in mod_authnz_ldap
- CVE-2017-3169 (HIGH): mod_ssl input validation flaw
- CVE-2017-7668 (MEDIUM): Weak htpasswd parameter validation
- CVE-2017-7679 (HIGH): mod_mime buffer overflow (RCE)
- CVE-2017-9788 (HIGH): OptionsBleed memory disclosure
- CVE-2016-4979 (MEDIUM): mod_auth_digest insufficient randomness

Device: 192.168.1.156