Firmware Security Audit Report

NYARC - Nyarime Advanced Reverse-engineering Console

Nyarc Professional v1.2.0

Firmware	BusyBox
Vendor	NETGEAR
Sample	nyarc-audit-generic-4209484294/rootfs
Size	218.9MB
Scan Date	2026-04-23 06:27:38
Tool	Nyarc Professional v1.2.0

RISK SCORE: 53/100 (MEDIUM)

Findings: 2 Critical, 8 High, 111 Medium, 241 Info

Findings Overview

#	Severity	CVSS	Finding
1	CRITICAL	5.3	OpenSSL libcrypto.so.1.0.0 â€” EOL
2	CRITICAL	7.5	OpenSSL 1.0.0 â€” EOL
3	HIGH	5.3	Zyxel backdoor detected (CVE-2024-40891): Shell command execution wrapper (3x)
4	HIGH	5.3	Ruijie backdoor detected (CVE-2023-34644): Module call command execution inte...
5	HIGH	5.3	Ivanti backdoor detected (CVE-2025-0282): Ivanti VPN appliance (CVE-2025-0282) (2x)
6	HIGH	5.3	Zyxel backdoor detected (CVE-2024-40891): CLI command handler (telnet injecti... (2x)
7	MEDIUM	5.3	D-Link/Tenda potential vulnerability: System command execution wrapper (commo... (50x)
8	MEDIUM	7.5	D-Link potential vulnerability: Firmware ZIP password derived from model name (50x)
9	MEDIUM	5.3	Generic potential vulnerability: Unbounded gets() input (critical overflow) (10x)
10	MEDIUM	5.3	Generic potential vulnerability: Default admin credentials

Detailed Findings

NYARC-001 | CRITICAL | CVSS 5.3

OpenSSL libcrypto.so.1.0.0 â€” EOL

Description: OpenSSL 1.0.x is EOL since 2020, multiple known CVEs including RCE

Evidence: /lib/libcrypto.so.1.0.0

NYARC-002 | CRITICAL | CVSS 7.5

OpenSSL 1.0.0 â€” EOL

Description: OpenSSL 1.0.x is EOL since 2020, multiple known CVEs including RCE

Evidence: /lib/libssl.so.1.0.0

NYARC-003 | HIGH | CVSS 5.3

Zyxel backdoor detected (CVE-2024-40891): Shell command execution wrapper

Description: Shell command execution wrapper

Evidence: /lib/libcms_cli.so

Solution: Update firmware. Add command filtering in cmsCli_run. Block pipe, semicolon, ampersand in telnet input.

CVE: CVE-2024-40891

NYARC-004 | HIGH | CVSS 5.3

Ruijie backdoor detected (CVE-2023-34644): Module call command execution interface

Description: Module call command execution interface

Evidence: /lib/libldb.so.1

Solution: Update to firmware v219+. Add input filtering in noauth.lua merge function. Filter , $(), backtick characters.

CVE: CVE-2023-34644

NYARC-005 | HIGH | CVSS 5.3

Ivanti backdoor detected (CVE-2025-0282): Ivanti VPN appliance (CVE-2025-0282)

Description: Ivanti VPN appliance (CVE-2025-0282)

Evidence: /www/Netgear_TNC_Italian.htm

Solution: Patch Ivanti Connect Secure immediately.

CVE: CVE-2025-0282

NYARC-006 | HIGH | CVSS 5.3

Zyxel backdoor detected (CVE-2024-40891): CLI command handler (telnet injection CVE-2024-40891)

Description: CLI command handler (telnet injection CVE-2024-40891)

Evidence: /bin/consoled_brcm

Solution: Update firmware. Add command filtering in cmsCli_run. Block pipe, semicolon, ampersand in telnet input.

CVE: CVE-2024-40891

NYARC-007 | MEDIUM | CVSS 5.3

D-Link/Tenda potential vulnerability: System command execution wrapper (common injection target)

Description: System command execution wrapper (common injection target)

Evidence: /lib/libcms_dal.so

Solution: Review this component for proper input validation and access control.

NYARC-008 | MEDIUM | CVSS 7.5

D-Link potential vulnerability: Firmware ZIP password derived from model name

Description: Firmware ZIP password derived from model name

Evidence: /etc/bdupd_start.sh

Solution: Review this component for proper input validation and access control.

NYARC-009 | MEDIUM | CVSS 5.3

Generic potential vulnerability: Unbounded gets() input (critical overflow)

Description: Unbounded gets() input (critical overflow)

Evidence: /lib/libcrypto.so

Solution: Replace gets() with fgets(). Never use gets().

NYARC-010 | MEDIUM | CVSS 5.3

Generic potential vulnerability: Default admin credentials

Description: Default admin credentials

Evidence: /usr/sbin/httpd

Solution: Review this component for proper input validation and access control.