



FIRMWARE ANALYSIS AND COMPARISON TOOL

Firmware Analysis of Netgear WNR2000v5 v. 1.0.0.28

HID	Netgear WNR2000v5 v. 1.0.0.28
Device Name	WNR2000v5
Vendor	Netgear
Device Class	Routers
Version	1.0.0.28
Release Date	1970-01-01
Size	3.46 MiB (3,629,189 Byte)

Unpacker (v. 0.7)

Plugin	generic_carver
Extracted	2
Output:	<p>DECIMAL HEXADECIMAL DESCRIPTION</p> <hr/> <p>128 0x80 ulmage header, header size: 64 bytes, header CRC: 0xA4E61569, created: 2014-12-23 07:39:28, image size: 851776 bytes, Data Address: 0x80002000, Entry Point: 0x801F68F0, data CRC: 0x568028C9, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "MIPS OpenWrt Linux-2.6.31"</p> <p>192 0xC0 LZMA compressed data, properties: 0x6D, dictionary size: 83886 08 bytes, uncompressed size: 2580544 bytes</p> <p>852032 0xD0040 ulmage header, header size: 64 bytes, header CRC: 0x7030BE3, created: 2014-12-23 07:39:29, image size: 2777092 bytes, Data Address: 0x80002000, Entry Point: 0x801F68F0, data CRC: 0xCC27EEB2, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "MIPS OpenWrt Linux-2.6.31"</p> <p>852096 0xD0080 Squashfs filesystem, little endian, version 4.0, compression: lzma, size: 2771667 bytes, 1143 inodes, blocksize: 131072 bytes, created: 2014-12-23 07:39:27</p>
Entropy	0.89

File Type (v. 1.0)

File Type	data
MIME	application/octet-stream
Containing Files	application/octet-stream (144) application/x-dbt (2) application/x-dosdriver (62) application/x-executable (134) application/x-lzma (1) application/x-object (43) application/x-sharedlib (27) filesystem/squashfs (1) image/gif (28) image/jpeg (3) image/png (3) image/x-icon (1) inode/symlink (41) text/plain (721)

Software Components (v. 0.4.1)

Time of Analysis	2020-05-20 13:46:10
Plugin Version	0.4.1
Summary	BusyBox 1.4.2 Dnsmasq 2.39 GNU Zebra 0.95a Linux Kernel 2.6.31 Netgear Smart Wizzard 3.2 OpenWrt 2.6.31 Point-to-Point Protocol daemon Point-to-Point Protocol daemon 2.4.3 hostapd 2.0 radvd radvd 1.5 udhcp 0.9.8

Users And Passwords (v. 0.4.4)

Time of Analysis	2020-05-20 13:46:10
Plugin Version	0.4.4
Summary	daemon fe80 nobody root

Crypto Material (v. 0.5.2)

Time of Analysis	2020-05-20 13:46:10
Plugin Version	0.5.2

Cpu Architecture (v. 0.3.2)

Time of Analysis	2020-05-20 13:46:11
Plugin Version	0.3.2
Summary	MIPS, 32-bit, big endian (M)

Hashes (v. 1.1)

md5	3a3a12eca3decc20e936ae6fe885da71
ripemd160	7e0f1f29c1ad27e81cba2b073c60b5c2456414cd
sha1	4de57fefafe00794485b37d8120c44d4c90bbe4b
sha256	1c842c3636191662a87b18d76766e141385b2714f9622ec98efaa82e78f6ad34
sha512	bc1c0864ed278428bb438062790a430d602e8a7903a785d4bad51f1145ebf 6cec8cb2c243907139f28d2e4613ab06d7d33247f8fcbd091234b692f8204ab3b4e

Cve Lookup (v. 0.0.4)

Time of Analysis	2020-05-20 13:46:24
Plugin Version	0.0.4
Summary	BusyBox 1.4.2 (CRITICAL) Dnsmasq 2.39 (CRITICAL) GNU Zebra 0.95a Linux Kernel 2.6.31 (CRITICAL) Netgear Smart Wizzard 3.2 OpenWrt 2.6.31 Point-to-Point Protocol daemon (CRITICAL) Point-to-Point Protocol daemon 2.4.3 (CRITICAL) hostapd 2.0

Exploit Mitigation (v. 0.1.2)

NX	NX disabled (144) NX enabled (60)
Canary	Canary disabled (204)
PIE	PIE - invalid ELF file (43) PIE disabled (134) PIE/DSO present (27)
RELRO	RELRO disabled (200) RELRO fully enabled (1) RELRO partially enabled (3)

Known Vulnerabilities (v. 0.2)

Time of Analysis	2020-05-20 13:46:24
Plugin Version	0.2

IPs and URIs (v. 0.4.2)

IPs v4	['1.0.0.28', '-35.0057, 138.7186']
IPs v6	list is empty
URIs	list is empty
Summary:	
1.0.0.28	

Binwalk (v. 0.5.2)

Signature Analysis:

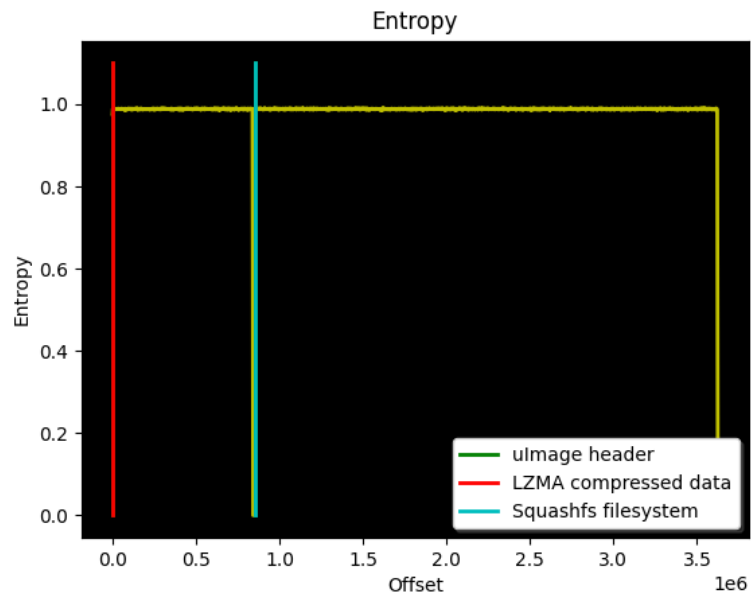
DECIMAL HEXADECIMAL DESCRIPTION

128 0x80 ulmage header, header size: 64 bytes, header CRC: 0xA4E61569, created: 2014-12-23 07:39:28, image size: 851776 bytes, Data Address: 0x80002000, Entry Point: 0x801F68F0, data CRC: 0x568028C9, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "MIPS OpenWrt Linux-2.6.31"

192 0xC0 LZMA compressed data, properties: 0x6D, dictionary size: 8388608 bytes, uncompressed size: 2580544 bytes

852032 0xD0040 ulmage header, header size: 64 bytes, header CRC: 0x7030BE3, created: 2014-12-23 07:39:29, image size: 2777092 bytes, Data Address: 0x80002000, Entry Point: 0x801F68F0, data CRC: 0xCC27EEB2, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "MIPS OpenWrt Linux-2.6.31"

852096 0xD0080 Squashfs filesystem, little endian, version 4.0, compression:lzma, size: 2771667 bytes, 1143 inodes, blocksize: 131072 bytes, created: 2014-12-23 07:39:27



Entropy Graph

Summary:

Squashfs filesystem
LZMA compressed data
ulmage header

Crypto Hints (v. 0.1)

Time of Analysis	2020-05-20 13:50:32
Plugin Version	0.1

Init Systems (v. 0.4.1)

Time of Analysis	2020-05-20 13:50:32
Plugin Version	0.4.1

Source Code Analysis (v. 0.4)

Time of Analysis	2020-05-20 13:50:32
Plugin Version	0.4

Input Vectors (v. 0.1.1)

Time of Analysis	2020-05-20 13:50:32
Plugin Version	0.1.1