SHA256: 83b1f0d1f806d8848ccfec16930821bbbb1eff4d1fa4b85a905403eaf8cddd18

File name: ignition-gateway

Detection ratio: 0 / 54

Analysis date: 2016-03-01 22:05:47 UTC (10 minutes ago)

The file being studied is an ELF! More specifically, it is a EXEC (Executable file) ELF for Unix systems running on Intel 80386 machines.

ELF Header

Class	ELF32
Data	2's complement, little endian
Header version	1 (current)
OS ABI	UNIX - System V
ABI version	0
Object file type	EXEC (Executable file)
Required architecture	Intel 80386
Object file version	0x1
Program headers	7
Section headers	26

ELF sections

Name	Type	Address	Offset	Size	Flags
	NULL	0x00000000	0x00000000	0	
.interp	PROGBITS	0x08048114	0x00000114	19	A
.note.ABI-tag	NOTE	0x08048128	0x00000128	32	A
.hash	HASH	0x08048148	0x00000148	1836	A
.dynsym	DYNSYM	0x08048874	0x00000874	4160	A
.dynstr	STRTAB	0x080498b4	0x000018b4	3346	A
.gnu.version	VERSYM	0x0804a5c6	0x000025c6	520	A
.gnu.version_r	VERNEED	0x0804a7d0	0x000027d0	144	A
.rel.dyn	REL	0x0804a860	0x00002860	1024	A
.rel.plt	REL	0x0804ac60	0x00002c60	992	A

Show all

ELF Segments

[+] PHDR ()

[+] INTERP ()

[+] LOAD ()

[+] LOAD ()

[+] DYNAMIC ()

[+] NOTE ()

[+] GNU_STACK ()

Shared libraries

libm.so.6

libpthread.so.0

libc.so.6

Imported symbols

pthread_detach *(FUNC)*

readlink *(FUNC)*

nl_langinfo *(FUNC)*

towlower *(FUNC)*

rename *(FUNC)*

sigaction *(FUNC)*

strchr *(FUNC)*

wcsrchr *(FUNC)*

getpid *(FUNC)*

nanosleep *(FUNC)*

Show all

Exported symbols

sysLogRemoteOk *(OBJECT)*

wrapperData *(OBJECT)*

consoleFlush *(OBJECT)*

queueMessages *(OBJECT)*

keyChars *(OBJECT)*

sysLogRemotePort *(OBJECT)*

currentLoginfoLevel *(OBJECT)*

previousNow *(OBJECT)*

logFileLastNowDate *(OBJECT)*

defaultLoginfoSourceName *(OBJECT)*

Show all

ExifTool file metadata

MIMEType	application/octet-stream
CPUByteOrder	Little endian
CPUArchitecture	32 bit
FileType	ELF executable
ObjectFileType	Executable file
CPUType	i386