Barco wePresent Global Hardcoded Root SSH Password

Authored by 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 a hardcoded root password hash included in the firmware image.

tags | exploit, root
advisories | CVE-2020-28334
SHA-256 | 75cc1a2f773099f090db6e25b10a5322af43049d1ef7d2035e513c189b3011ed

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
KL-001-2020-008 : Barco wePresent Global Hardcoded Root SSH Password

Title: Barco wePresent Global Hardcoded Root SSH Password
Advisory ID: KL-001-2020-008
Publication Date: 2020.11.20
Publication URL: https://korelogic.com/Resources/Advisories/KL-001-2020-008.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-798: Use of Hard-coded Credentials
     CVE ID: CVE-2020-28334


2. Vulnerability Description

     The Barco wePresent device has a hardcoded root password hash
     included in the firmware image. To our knowledge the password
     hash has not been cracked and published; it is possible this
     could occur at any time. This combined with KL-001-2020-004
     (CVE-2020-28329), KL-001-2020-005 (CVE-2020-28330), and
     KL-001-2020-007 (CVE-2020-28331) could be used in a simple
     and automated exploit chain to go from unauthenticated remote
     attacker to root shell.


3. Technical Description

     In looking at the unpacked firmware, a root hash was quickly
     identified in the /etc/shadow file on the device. It is the
     only account in the /etc/shadow. The device does not prompt
     the administrator to set a new root password, therefore this
     password is hardcoded and exists across all devices.


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) 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.
     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

     After unpacking the firmware:
     $ ls -al etc/shadow
     -rwxr-xr-x 1 user user 59 May 25 00:11 etc/shadow

     $ cat etc/shadow
     root:$1$reqE8o6b$[REDACTED]:12940:0:99999:7:::


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
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

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
nu11secur1ty	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	(6,926)
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	(1,690)
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)

- Spoof (2,166)
- SQL Injection (16,102)
- TCP (2,379)
- Trojan (686)
- UDP (876)
- Virus (662)
- Vulnerability (31,136)
- Web (9,365)
- Whitepaper (3,729)
- x86 (946)
- XSS (17,494)
- Other

- SUSE (1,444)
- Ubuntu (8,199)
- UNIX (9,159)
- UnixWare (185)
- Windows (6,511)
- Other

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