

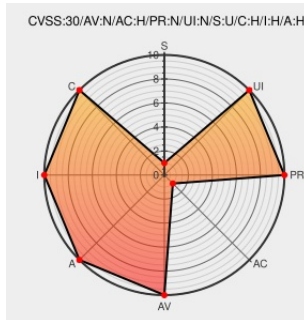


CVE-2018-20219

Published on: 03/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:36 PM UTC

CVE-2018-20219

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Enc-400 Hdmi](#) from [Teracue](#) contain the following vulnerability:

An issue was discovered on Teracue ENC-400 devices with firmware 2.56 and below. After successful authentication, the device sends an authentication cookie to the end user such that they can access the devices web administration panel. This token is hard-coded to a string in the source code (/usr/share/www/check.lp file). By setting this cookie in a browser, an attacker is able to maintain access to every ENC-400 device without knowing the password, which results in authentication bypass. Even if a user changes the password on the device, this token is static and unchanged.

CVE-2018-20219 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
-------------	------	------

Teracue ENC-400 Command Injection / Missing Authentication ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/151802/Teracue-ENC-400-Command-Injection-Missing-Authentication.html
ZX Security Limited - Information Security Consultants	Not Applicable web.archive.org text/html Inactive Link Not Archived	 MISC zxsecurity.co.nz/research.html
Full Disclosure: Multiple issues in Teracue ENC-400 including pre-authenticated remote code execution	Mailing List Third Party Advisory seclists.org text/html	 MISC seclists.org/fulldisclosure/2019/Feb/48

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Teracue	Enc-400 Hdmi	-	All	All	All
Hardware 	Teracue	Enc-400 Hdmi	-	All	All	All
Hardware 	Teracue	Enc-400 Hdmi2	-	All	All	All
Hardware 	Teracue	Enc-400 Hdmi2	-	All	All	All
Operating System	Teracue	Enc-400 Hdmi2 Firmware	All	All	All	All
Operating System	Teracue	Enc-400 Hdmi Firmware	All	All	All	All
Hardware 	Teracue	Enc-400 Hdsdi	-	All	All	All
Hardware 	Teracue	Enc-400 Hdsdi	-	All	All	All
Operating System	Teracue	Enc-400 Hdsdi Firmware	All	All	All	All

```
cpe:2.3:h:teracue:enc-400 hdmi:-:~::~::~:
```

```
cpe:2.3:h:teracue:enc-400 hdmi:-:*:*:*:*:*:
```

```
cpe:2.3:h:teracue:enc-400 hdmi2:-:~::~:~::~:~::~:~::~:~::~:
```

```
cpe:2.3:h:teracue:enc-400 hdmi2:-:~::~:~::~:~::~:~::~:~::~:
```

```
cpe:2.3:o:teracue:enc-400 hdmi2 firmware:*.***.***.***.
```

```
cpe:2.3:o:teracue:enc-400 hdmi firmware:*:*:*:*:*:*:
```

```
cpe:2.3:h:teracue:enc-400_hdsdi:-:*****:
```

```
cpe:2.3:h:teracue:enc-400_hdsdi:-:*****:
```

```
cpe:2.3:o:teracue:enc-400_hdsdi_firmware:*****:
```

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report