



CVE-2020-10633

Published on: 04/07/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:34 PM UTC

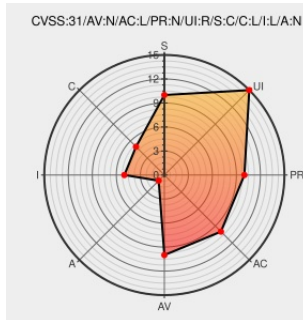
CVE-2020-10633

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ewon Cosy](#) from [Hms-networks](#) contain the following vulnerability:

A non-persistent XSS (cross-site scripting) vulnerability exists in eWON Flexy and Cosy (all firmware versions prior to 14.1s0). An attacker could send a specially crafted URL to initiate a password change for the device. The target must introduce the credentials to the gateway before the attack can be successful.

CVE-2020-10633 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
HMS Networks eWON Flexy and Cosy CISA	Third Party Advisory US Government Resource www.us-cert.gov	MISC www.us-cert.gov/ics/advisories/icsa-20-098-03

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 	Hms-networks	Ewon Cosy	-	All	All	All
Hardware 	Hms-networks	Ewon Cosy	-	All	All	All
Operating System	Hms-networks	Ewon Cosy Firmware	All	All	All	All
Operating System	Hms-networks	Ewon Cosy Firmware	All	All	All	All
Hardware 	Hms-networks	Ewon Flexy	-	All	All	All
Hardware 	Hms-networks	Ewon Flexy	-	All	All	All
Operating System	Hms-networks	Ewon Flexy Firmware	All	All	All	All
Operating System	Hms-networks	Ewon Flexy Firmware	All	All	All	All

```
cpe:2.3:h:hms-networks:ewon_cosy:-:*:*:*:*:*:*:*:
```

```
cpe:2.3:h:hms-networks:ewon_cosy:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:hms-networks:ewon_cosy_firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:hms-networks:ewon cosy firmware:*:*:*:*:*:*:
```

```
cpe:2.3:h:hms-networks:ewon flexy:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:hms-networks:ewon flexy:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:hms-networks:ewon flexy firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:hms-networks:ewon flexy firmware:*.:.:.:.:.:.:
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)