



# CVE-2021-27442

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-27442
<b>State</b>	PUBLIC
<b>Assigner</b>	ics-cert@hq.dhs.gov
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-05-16 18:15:00 UTC
<b>Updated</b>	2022-05-25 16:22:00 UTC
<b>Description</b>	The Weintek cMT product line is vulnerable to a cross-site scripting vulnerability, which could allow an unauthenticated rem

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-ctrl01</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-ctrl01 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-fhd</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-fhd Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-g01</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-g01 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-g02</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-g02 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-g03</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-g03 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-g04</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-g04 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-hdm</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-hdm Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-svr-100</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-svr-100 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-svr-102</a>	-	All	All	All

Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-svr-102 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-svr-200</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-svr-200 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt-svr-202</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt-svr-202 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt3071</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt3071 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt3072</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt3072 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt3090</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt3090 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt3103</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt3103 Firmware</a>	All	All	All	All
Hardware	<a href="#">Weintek</a>	<a href="#">Cmt3151</a>	-	All	All	All
Operating System	<a href="#">Weintek</a>	<a href="#">Cmt3151 Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="https://dl.weintek.com/public/Document/TEC/TEC21001E_cMT_EasyWeb_V1_Security_Issues.pdf">dl.weintek.com/public/Document/TEC/TEC21001E_cMT_EasyWeb_V1_Security_Issues.pdf</a>	CONFIRM	<a href="https://dl.weintek.com">dl.weintek.com</a>	
Weintek EasyWeb cMT   CISA	MISC	<a href="https://www.cisa.gov">www.cisa.gov</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analy

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Marcin Dudek from CERT.PL reported these vulnerabilities to CISA.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](https://status.cve.report)