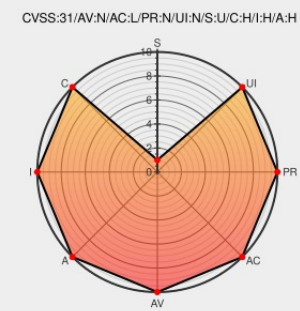
CVE-2021-33352

Published on: Not Yet Published

Last Modified on: 03/14/2023 08:13:00 PM UTC

CVE-2021-33352

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Help Desk from Wyomind contain the following vulnerability:

An issue in Wyomind Help Desk Magento 2 extension v.1.3.6 and before fixed in v.1.3.7 allows attacker to execute arbitrary code via a phar file upload in the ticket message field.

CVE-2021-33352 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
Wyomind Help Desk 1.3.6 - Remote Code Execution (RCE) - Multiple webapps Exploit	www.exploit-db.com, Proof of Concept, text/html	MISC www.exploit-db.com/exploits/50113
Magento 2 - Helpdesk / Support - Extension for Magento	www.wyomind.com, text/html	MISC www.wyomind.com/magento2/helpdesk-magento-2.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wyomind	Help Desk	All	All	All	All

cpe:2.3:a:wyomind:help_desk:*:*:*:*:*:magento_2:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-33352 : An issue in Wyomind Help Desk Magento 2 extension v.1.3.6 and before fixed in v.1.3.7 allows attac… twitter.com/i/web/status/1…	2023-03-08 22:07:43
/r/netcve	CVE-2021-33352	2023-03-08 23:38:25

← Previous ID

Next ID→