



CVE-2022-32763

Published on: Not Yet Published

Last Modified on: 12/19/2022 02:33:00 PM UTC

CVE-2022-32763

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:30/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H



Certain versions of [Lansweeper](#) from [Lansweeper](#) contain the following vulnerability:

A cross-site scripting (xss) sanitization vulnerability bypass exists in the SanitizeHtml functionality of Lansweeper lansweeper 10.1.1.0. A specially-crafted HTTP request can lead to arbitrary Javascript code injection. An attacker can send an HTTP request to trigger this vulnerability.

CVE-2022-32763 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Cisco](#) **Lansweeper** - lansweeper version = 10.1.1.0

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

CVE References

Description	Tags	Link
TALOS-2022-1541 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2022-1541

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](#).

Related QID Numbers

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lansweeper	Lansweeper	10.1.1.0	All	All	All
cpe:2.3:a:lansweeper:lansweeper:10.1.1.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-32763 : A cross-site scripting xss sanitization vulnerability bypass exists in the SanitizeHtml function... twitter.com/i/web/status/1...	2022-12-15 09:40:03
 /r/netcve	CVE-2022-32763	2022-12-15 10:41:04

[← 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](#)