



CVE-2023-2521

Published on: Not Yet Published

Last Modified on: 10/23/2023 06:10:17 AM UTC

CVE-2023-2521

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

Certain versions of [Next-7004n](#) from [Ez-net](#) contain the following vulnerability:

A vulnerability was found in NEXTU NEXT-7004N 3.0.1. It has been classified as problematic. Affected is an unknown function of the file /boafm/formFilter of the component POST Request Handler. The manipulation of the argument url with the input `<svg onload=alert(1337)>` leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-228012. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

CVE-2023-2521 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **NEXTU - NEXT-7004N** version = 3.0.1

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
Login required	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?ctiid.228012
CVE-2023-2521: NEXTU NEXT-7004N POST Request formFilter cross site scripting	vuldb.com text/html	MISC vuldb.com/?id.228012

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

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or correct 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 	Ez-net	Next-7004n	-	All	All	All
Operating System	Ez-net	Next-7004n Firmware	3.0.1	All	All	All
cpe:2.3:h:ez-net:next-7004n:-:*:*:*:*:*:						
cpe:2.3:o:ez-net:next-7004n_firmware:3.0.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-2521 : A vulnerability was found in NEXTU NEXT-7004N 3.0.1. It has been classified as problematic. Affecte... twitter.com/i/web/status/1...	2023-05-04 17:08:30
 @threatmeter	CVE-2023-2521 NEXTU NEXT-7004N 3.0.1 POST Request /boafrm/formFilter url cross site scripting A vulnerability was... twitter.com/i/web/status/1...	2023-05-04 18:50:59

[← Previous ID](#)

[Next ID →](#)