



# CVE-2020-23591

Published on: Not Yet Published

Last Modified on: 11/23/2022 08:53:00 PM UTC

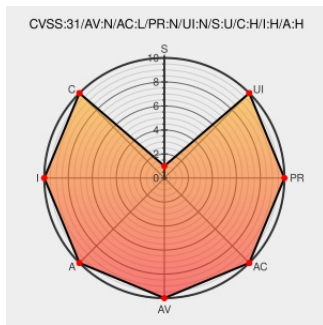
## CVE-2020-23591

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Op-xt71000n](#) from [Optilinknetwork](#) contain the following vulnerability:

A vulnerability in OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP\_V3.3.1-191028 allows an attacker to upload arbitrary files through " /mgm\_dev\_upgrade.asp " which can "delete every file for Denial of Service (using 'rm -rf \*.\*' in the code), reverse connection (using '.asp' webshell), backdoor.

CVE-2020-23591 has been assigned by [M](#) [cve@mitre.org](mailto: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
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

## CVE References


Description	Tags	Link
GitHub - <a href="#">huzaiyahussain98/CVE-2020-23591</a> : ARBITAR FILE UPLOAD LEADS TO "delete every file for Denial of Service (using 'rm -rf *.*' in the code), reverse connection (using '.asp' webshell), backdoor , Escalation of Privileges, etc".	<a href="#">github.com</a> <a href="#">text/html</a>	<a href="#">MISC</a> <a href="https://github.com/huzaiyahussain98/CVE-2020-23591">github.com/huzaiyahussain98/CVE-2020-23591</a>

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](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE




ARBITAR FILE UPLOAD LEADS TO "delete every file for Denial of Service (using 'rm -rf \*.\*' in the code), reverse conne...

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	<a href="#">Optilinknetwork</a>	<a href="#">Op-xt71000n</a>	2.2	All	All	All
Operating System	<a href="#">Optilinknetwork</a>	<a href="#">Op-xt71000n Firmware</a>	3.3.1-191028	All	All	All
cpe:2.3:h:optilinknetwork:op-xt71000n:2.2:*:*:*:*:*:						
cpe:2.3:o:optilinknetwork:op-xt71000n_firmware:3.3.1-191028:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-23591 : A vulnerability in OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP_V3.3.1-19102... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-11-23 02:03:28
 @JohnJasonFallow	New vulnerability on the NVD: CVE-2020-23591 <a href="https://ift.tt/Yl6rwMW">ift.tt/Yl6rwMW</a>	2022-11-23 06:16:54
 /r/netcve	<a href="#">CVE-2020-23591</a>	2022-11-23 03:38:47

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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](#)