

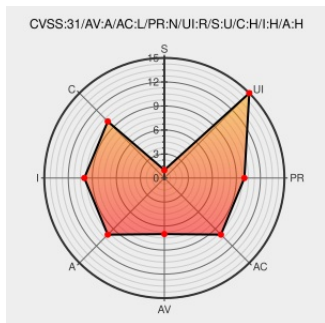


CVE-2022-4098

Published on: Not Yet Published

Last Modified on: 03/31/2023 04:12:00 PM UTC

CVE-2022-4098 - advisory for VDE-2022-057

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

Certain versions of [Com-server 20ma](#) from [Wut](#) contain the following vulnerability:

Multiple Wiesemann&Theis products of the ComServer Series are prone to an authentication bypass through IP spoofing. After a user logged in to the WBM of the Com-Server an unauthenticated attacker in the same subnet can obtain the session ID and through IP spoofing change arbitrary settings by crafting modified HTTP Get requests. This may result in a complete takeover of the device.

CVE-2022-4098 has been assigned by [cert](#) info@cert.vde.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8 - HIGH**

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

CVE References

Description	Tags	Link
VDE-2022-057 CERT@VDE	cert.vde.com text/html	MISC cert.vde.com/en/advisories/VDE-2022-057/

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](#).

There are currently no QIDs associated with this CVE

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware  	Wut	Com-server 20ma	-	All	All	All
Operating System	Wut	Com-server 20ma Firmware	All	All	All	All
Hardware  	Wut	Com-server Highspeed 100basefx	-	All	All	All
Operating System	Wut	Com-server Highspeed 100basefx Firmware	All	All	All	All
Hardware  	Wut	Com-server Highspeed 100baseLx	-	All	All	All
Operating System	Wut	Com-server Highspeed 100baseLx Firmware	All	All	All	All
Hardware  	Wut	Com-server Highspeed 19 1port	-	All	All	All
Operating System	Wut	Com-server Highspeed 19 1port Firmware	All	All	All	All
Hardware  	Wut	Com-server Highspeed 19 4port	-	All	All	All
Operating System	Wut	Com-server Highspeed 19 4port Firmware	All	All	All	All
Hardware  	Wut	Com-server Highspeed Compact	-	All	All	All
Operating System	Wut	Com-server Highspeed Compact Firmware	All	All	All	All
Hardware  	Wut	Com-server Highspeed Industry	-	All	All	All
Operating System	Wut	Com-server Highspeed Industry Firmware	All	All	All	All
Hardware  	Wut	Com-server Highspeed Isolated	-	All	All	All
Operating System	Wut	Com-server Highspeed Isolated Firmware	All	All	All	All
Hardware  	Wut	Com-server Highspeed Lc	-	All	All	All
Operating System	Wut	Com-server Highspeed Lc Firmware	All	All	All	All
Hardware  	Wut	Com-server Highspeed Oem	-	All	All	All
Operating System	Wut	Com-server Highspeed Oem Firmware	All	All	All	All
Hardware  	Wut	Com-server Highspeed Office 1port	-	All	All	All
Operating System	Wut	Com-server Highspeed Office 1port Firmware	All	All	All	All

Hardware		Wut	Com-server Highspeed Office 4port	-	All	All	All
Operating System		Wut	Com-server Highspeed Office 4port Firmware	All	All	All	All
Hardware		Wut	Com-server Highspeed Poe	-	All	All	All
Hardware		Wut	Com-server Highspeed Poe 3x Isolated	-	All	All	All
Operating System		Wut	Com-server Highspeed Poe 3x Isolated Firmware	All	All	All	All
Operating System		Wut	Com-server Highspeed Poe Firmware	All	All	All	All
Hardware		Wut	Com-server Highspeed UI	-	All	All	All
Operating System		Wut	Com-server Highspeed UI Firmware	All	All	All	All
Hardware		Wut	Com-server	-	All	All	All
Operating System		Wut	Com-server Firmware	All	All	All	All
cpe:2.3:h:wut:com-server_20ma:-:*:*:*:*:*:							
cpe:2.3:o:wut:com-server_20ma_firmware:*:*:*:*:*:							
cpe:2.3:h:wut:com-server_highspeed_100basefx:-:*:*:*:*:*:							
cpe:2.3:o:wut:com-server_highspeed_100basefx_firmware:*:*:*:*:*:							
cpe:2.3:h:wut:com-server_highspeed_100baselx:-:*:*:*:*:*:							
cpe:2.3:o:wut:com-server_highspeed_100baselx_firmware:*:*:*:*:*:							
cpe:2.3:h:wut:com-server_highspeed_19\"_1port:-:*:*:*:*:*:							
cpe:2.3:o:wut:com-server_highspeed_19\"_1port_firmware:*:*:*:*:*:							
cpe:2.3:h:wut:com-server_highspeed_19\"_4port:-:*:*:*:*:*:							
cpe:2.3:o:wut:com-server_highspeed_19\"_4port_firmware:*:*:*:*:*:							
cpe:2.3:h:wut:com-server_highspeed_compact:-:*:*:*:*:*:							
cpe:2.3:o:wut:com-server_highspeed_compact_firmware:*:*:*:*:*:							
cpe:2.3:h:wut:com-server_highspeed_industry:-:*:*:*:*:*:							
cpe:2.3:o:wut:com-server_highspeed_industry_firmware:*:*:*:*:*:							
cpe:2.3:h:wut:com-server_highspeed_isolated:-:*:*:*:*:*:							
cpe:2.3:o:wut:com-server_highspeed_isolated_firmware:*:*:*:*:*:							
cpe:2.3:h:wut:com-server_highspeed_lc:-:*:*:*:*:*:							
cpe:2.3:o:wut:com-server_highspeed_lc_firmware:*:*:*:*:*:							

cpe:2.3:h:wut:com-server_highspeed_oem:-:*:*:*:*:*:
cpe:2.3:o:wut:com-server_highspeed_oem_firmware:*:*:*:*:*:
cpe:2.3:h:wut:com-server_highspeed_office_1port:-:*:*:*:*:*:
cpe:2.3:o:wut:com-server_highspeed_office_1port_firmware:*:*:*:*:*:
cpe:2.3:h:wut:com-server_highspeed_office_4port:-:*:*:*:*:*:
cpe:2.3:o:wut:com-server_highspeed_office_4port_firmware:*:*:*:*:*:
cpe:2.3:h:wut:com-server_highspeed_poe:-:*:*:*:*:*:
cpe:2.3:h:wut:com-server_highspeed_poe_3x_isolated:-:*:*:*:*:*:
cpe:2.3:o:wut:com-server_highspeed_poe_3x_isolated_firmware:*:*:*:*:*:
cpe:2.3:o:wut:com-server_highspeed_poe_firmware:*:*:*:*:*:
cpe:2.3:h:wut:com-server_highspeed_ul:-:*:*:*:*:*:
cpe:2.3:o:wut:com-server_highspeed_ul_firmware:*:*:*:*:*:
cpe:2.3:h:wut:com-server_\+ -:*:*:*:*:*:
cpe:2.3:o:wut:com-server_\+ +_firmware:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-4098 : Multiple Wiesemann&Theis products of the ComServer Series are prone to an authentication bypass thr... twitter.com/i/web/status/1...	2022-12-13 08:01:41
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-4098 Multiple Wiesemann&Theis products of the ComServer Series are pron... twitter.com/i/web/status/1...	2022-12-13 08:55:55
 r/netcve	CVE-2022-4098	2022-12-13 09:39:24

[← 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