



CVE-2021-4105

Published on: Not Yet Published

Last Modified on: 07/07/2023 07:20:00 PM UTC

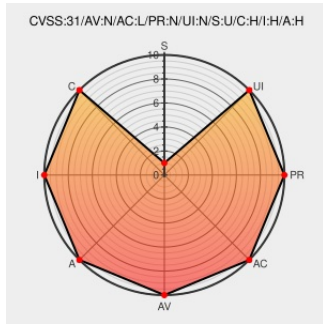
CVE-2021-4105 - advisory for TR-23-0108

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Coslat Bx5s1d3](#) from [Bg-tek](#) contain the following vulnerability:

Improper Handling of Parameters vulnerability in BG-TEK COSLAT Firewall allows Remote Code Inclusion. This issue affects COSLAT Firewall: from 5.24.0.R.20180630 before 5.24.0.R.20210727.

CVE-2021-4105 has been assigned by cve@usom.gov.tr to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [BG-TEK](#) - **COSLAT Firewall** version < 5.24.0.r.20210727

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
Ulusal Siber Olaylara Müdahale Merkezi - USOM	www.usom.gov.tr text/html	MISC www.usom.gov.tr/bildirim/tr-23-0108
ÖNEMLİ: Kritik Güncelleme - 27-07-2021 tarihinde yayınlanan güncelleme içeriği ~ Coslat Firewall Blog	blog.coslat.com text/html	MISC blog.coslat.com/2021/07/onemli-kritik-guncelleme-2021-07-27.html

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Bg-tek	Coslat Bx5s1d3	-	All	All	All
Operating System	Bg-tek	Coslat Bx5s1d3 Firmware	All	All	All	All
Hardware 	Bg-tek	Coslat Bx5s1d4	-	All	All	All
Operating System	Bg-tek	Coslat Bx5s1d4 Firmware	All	All	All	All
Hardware 	Bg-tek	Coslat Bx5s1d5	-	All	All	All
Operating System	Bg-tek	Coslat Bx5s1d5 Firmware	All	All	All	All
Hardware 	Bg-tek	Coslat Rm1ds1000	-	All	All	All
Operating System	Bg-tek	Coslat Rm1ds1000 Firmware	All	All	All	All
Hardware 	Bg-tek	Coslat Rm2ds2000	-	All	All	All
Operating System	Bg-tek	Coslat Rm2ds2000 Firmware	All	All	All	All
Hardware 	Bg-tek	Coslat Rm2s200	-	All	All	All
Operating System	Bg-tek	Coslat Rm2s200 Firmware	All	All	All	All
Hardware 	Bg-tek	Coslat Rm3s300	-	All	All	All
Operating System	Bg-tek	Coslat Rm3s300 Firmware	All	All	All	All
Hardware 	Bg-tek	Coslat Rm4s500	-	All	All	All
Operating System	Bg-tek	Coslat Rm4s500 Firmware	All	All	All	All

cpe:2.3:h:bg-tek:coslat_bx5s1d3:-:*:*:*:*:*:

cpe:2.3:o:bg-tek:coslat_bx5s1d3_firmware:*:*:*:*:*:

cpe:2.3:h:bg-tek:coslat_bx5s1d4:-:*:*:*:*:*:

cpe:2.3:o:bg-tek:coslat_bx5s1d4_firmware:*:*:*:*:*:

cpe:2.3:h:bg-tek:coslat_bx5s1d5:-:*:*:*:*:*:

cpe:2.3:o:bg-tek:coslat_bx5s1d5_firmware:*:*:*:*:*:



cpe:2.3:h:bg-tek:coslat_rm1ds1000:-:*:*:*:*:*:

cpe:2.3:o:bg-tek:coslat_rm1ds1000_firmware:*:*:*:*:*:

cpe:2.3:h:bg-tek:coslat_rm2ds2000:-:*:*:*:*:*:

cpe:2.3:o:bg-tek:coslat_rm2ds2000_firmware:~::~::~::~:
cpe:2.3:h:bg-tek:coslat_rm2s200:-~::~::~::~:
cpe:2.3:o:bg-tek:coslat_rm2s200_firmware:~::~::~::~::~:
cpe:2.3:h:bg-tek:coslat_rm3s300:-~::~::~::~:
cpe:2.3:o:bg-tek:coslat_rm3s300_firmware:~::~::~::~::~:
cpe:2.3:h:bg-tek:coslat_rm4s500:-~::~::~::~:
cpe:2.3:o:bg-tek:coslat_rm4s500_firmware:~::~::~::~::~:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-4105 : Improper Handling of Parameters vulnerability in BG-TEK COSLAT Firewall allows Remote Code Inclusio... twitter.com/i/web/status/1...	2023-02-24 12:09:52
 /r/netcve	CVE-2021-4105	2023-02-24 13:38:13

[← 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