



Missing Authorization Checks in LiderAhenk

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-3825
State	PUBLISHED
Assigner	TR-CERT
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-01 15:15:07 UTC
Updated	2026-05-18 09:16:22 UTC
Description	On 2.1.15 version and below of Lider module in LiderAhenk software is leaking it's configurations via an unsecured API. An

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-306 | CWE-306 CWE-306 Missing Authentication for Critical Function

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	iletisim@usom.gov.tr	Secondary	9.6	CRITICAL	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.6	CRITICAL	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pardus	Liderahenk	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TUBITAK	Lider	affected unspecified 2.1.16 custom	Not specified

References

Reference	Source	Link
siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-21-0795	iletisim@usom.gov.tr	siberguvenlik.gov.tr
LiderAhenk 0day – All your PARDUS Clients Belongs To Me – Pentest Blog	af854a3a-2127-422b-91ae-364da2661108	pentest.blog
Ulusal Siber Olaylara Müdahale Merkezi - USOM	af854a3a-2127-422b-91ae-364da2661108	www.usom.gov.tr
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Mehmet INCE from PRODAFT (en)

Additional Advisory Data

Solutions

CNA: Lider component should be updated to 2.1.16.

Exploits

CNA: <https://github.com/mdisec/pardus-liderahenk-0day-RCE>

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report