



# MAXHUB Pivot Client Application Use of a Broken or Risky Cryptographic Algorithm

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

## Summary

<b>CVE</b>	CVE-2026-6411
<b>State</b>	PUBLISHED
<b>Assigner</b>	icscert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 23:16:32 UTC
<b>Updated</b>	2026-05-07 23:16:32 UTC
<b>Description</b>	This vulnerability, in the MAXHUB Pivot client application versions prior to v1.36.2, may allow an attacker to obtain encrypted

## Risk And Classification

**Primary CVSS:** v3.1 7.3 HIGH from ics-cert@hq.dhs.gov

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

**Problem Types:** CWE-327 | CWE-327 CWE-327

Version	Source	Type	Score	Severity	Vector
3.1	ics-cert@hq.dhs.gov	Secondary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	CVSS	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	MAXHUB	MAXHUB Pivot Client Application	affected 1.36.2 custom	Not specified
CNA	MAXHUB	MAXHUB Pivot Client Application	unaffected 1.36.2	Not specified

#### References

Reference	Source	Link	Tags
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-12...	ics-cert@hq.dhs.gov	<a href="#">github.com</a>	
www.maxhub.com/en/support	ics-cert@hq.dhs.gov	<a href="#">www.maxhub.com</a>	
www.cisa.gov/news-events/ics-advisories/icsa-26-127-01	ics-cert@hq.dhs.gov	<a href="#">www.cisa.gov</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

#### Vendor Comments And Credit

##### Discovery Credit

**CNA:** Malik MAKKES and Yassine BENGANA of Abicom Groupe OCI reported this vulnerability to MAXHUB. (en)

#### Additional Advisory Data

##### Solutions

**CNA:** MAXHUB recommends users upgrade the Pivot client application to v1.36.2 or newer. The remediation has been made available through an OTA update. Users running v1.36.2 or later are not affected and need only ensure they continue to maintain the latest version. At this time, MAXHUB is not aware of any public exploitation of this issue. For more information, see the MAXHUB support page. <https://www.maxhub.com/en/support/>

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)