



# CVE-2023-37756

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

## Summary

<b>CVE</b>	CVE-2023-37756
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-14 21:15:00 UTC
<b>Updated</b>	2023-11-07 04:17:00 UTC
<b>Description</b>	I-doit pro 25 and below and I-doit open 25 and below employ weak password requirements for Administrator account creati

## Risk And Classification

**Problem Types:** CWE-521

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	I-doit	I-doit	All	All	All	All
Application	I-doit	I-doit	All	All	All	All

## References

Reference	Source
i-doit Pro v25 and below weak password & add-on upload to RCE, CVE-2023-37756   by Ray   Sep, 2023   Medium	
CVE-2023-37756 – Weak Password Requirement in admin-center lead to malicious plugin upload in the i-doit Pro 25 and below	MISC
i-doit Pro v25 and below weak password & add-on upload to RCE, CVE-2023-37756   by Ray   Sep, 2023   Medium	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](#)