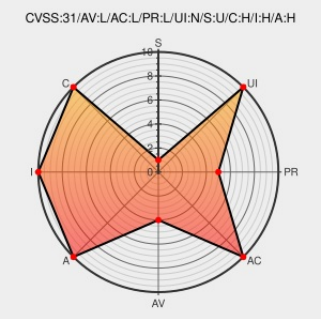
CVE-2017-20112

Published on: Not Yet Published

Last Modified on: 07/07/2022 06:59:00 PM UTC

CVE-2017-20112

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ivpn from Ivpn contain the following vulnerability:

A vulnerability has been found in IVPN Client 2.6.6120.33863 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument --up cmd leads to improper privilege management. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 2.6.2 is able to address this issue. It is recommended to upgrade the affected component.

CVE-2017-20112 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **IVPN** - **Client** version **2.6.6120.33863**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

Full Disclosure: IVPN Client for Windows 2.6.6120.33863 Privilege Escalation	seclists.org text/html	MISC seclists.org/fulldisclosure/2017/Feb/14
CVE-2017-20112 | IVPN Client privileges management	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?id.96655
exploits/ivpn_privilege_escalation.py at master · kacperszurek/exploits · GitHub	github.com text/html	MISC github.com/kacperszurek/exploits/blob/master/IVPN/ivpn_privilege_escalat

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
Application	Ivpn	Ivpn	2.6.6120.33863	All	All	All

cpe:2.3:a:ivpn:ivpn:2.6.6120.33863:*:*:*:*:windows:*:*:

Discovery Credit

Kacper Szurek

← Previous ID

Next ID→