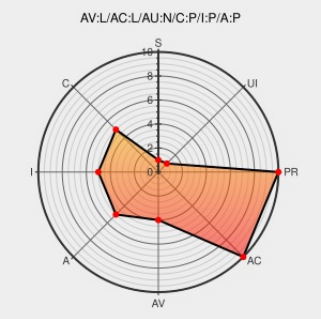
CVE-2002-1972

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 06/15/2021 12:00:00 AM UTC

CVE-2002-1972

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



Certain versions of Pp Powerswitch from Sebastian Dehne contain the following vulnerability:

Unknown vulnerability in Parallel port powerSwitch (aka pp_powerSwitch) 0.1 does not properly enforce access controls, which allows local users to access arbitrary ports.

CVE-2002-1972 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
pp_powerSwitch Access Control Bug May Let Remote Authenticated Users Control Any Port - SecurityTracker	Patch, securitytracker.com, text/html	SECTRACK 1005534
ISS X-Force Database: pp-powerswitch-port-access (10552): pp_powerSwitch could allow an attacker to control any port	Patch, web.archive.org, text/html, Inactive Link, Not Archived	XF pp-powerswitch-port-access(10552)
freshmeat.net: Parallel port powerSwitch 0.1.1	Patch, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM freshmeat.net/releases/101529/

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	Sebastian Dehne	Pp Powerswitch	0.1	All	All	All
Application	Sebastian Dehne	Pp Powerswitch	0.1	All	All	All

cpe:2.3:a:sebastian_dehne:pp_powerswitch:0.1:*:*:*:*:*:*:*:

cpe:2.3:a:sebastian_dehne:pp_powerswitch:0.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→