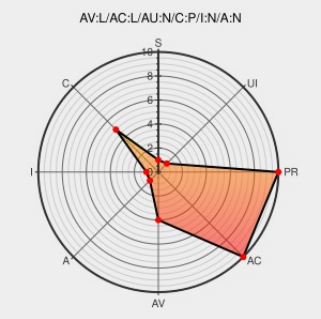
CVE-2002-1970

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

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1970

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



Certain versions of Snortcenter from Snortcenter contain the following vulnerability:

SnortCenter 0.9.5, when configured to push Snort rules, stores the rules in a temporary file with world-readable and world-writable permissions, which allows local users to obtain usernames and passwords for the alert database servers.

CVE-2002-1970 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
SnortCenter Insecure Sensor Configuration File Permissions Vulnerability	Patch, cve.report (archive), text/html	BID 6109
No Description Provided	Patch, online.securityfocus.com, Inactive Link, Not Archived	BUGTRAQ 20021105 SnortCenter 0.9.5 temp file naming problems...
ISS X-Force Database: snortcenter-tmp-file-insecure (10540): SnortCenter creates an insecure temporary file	Patch, web.archive.org, text/html, Inactive Link, Not Archived	XF snortcenter-tmp-file-insecure(10540)

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	Snortcenter	Snortcenter	0.9.5	All	All	All
Application	Snortcenter	Snortcenter	0.9.5	All	All	All

cpe:2.3:a:snortcenter:snortcenter:0.9.5:*:*:*:*:*:*:*:

cpe:2.3:a:snortcenter:snortcenter:0.9.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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