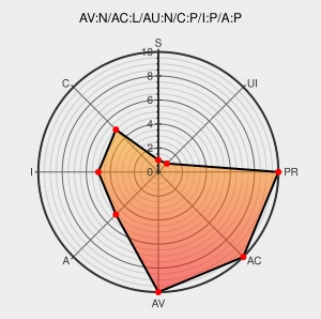
CVE-2004-0082

Published on: 03/03/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:12 PM UTC

CVE-2004-0082

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



Certain versions of Samba from Samba contain the following vulnerability:

The mksmbpasswd shell script (mksmbpasswd.sh) in Samba 3.0.0 and 3.0.1, when creating an account but marking it as disabled, may overwrite the user password with an uninitialized buffer, which could enable the account with a more easily guessable password.

CVE-2004-0082 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 3919
O-078: Samba - Unauthorized Access to SMB Accounts	web.archive.org text/html Inactive Link Not Archived	CIAC O-078
redhat.com | Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2004:064
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF samba-mksmbpasswd-gain-access(15132)
VuXML: Samba 3.0.x password initialization bug	www.vuxml.org	CONFIRM www.vuxml.org/freebsd/3388eff9-5d6e-

	text/html	11d8-80e3-0020ed76ef5a.html
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:827
Samba Mksmbpasswd.sh Insecure User Account Creation Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	BID 9637
Site not found (404)	us1.samba.org text/html Inactive Link Not Archived	CONFIRM us1.samba.org/samba/ftp/WHATSNEW-3.0.2a.txt

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	Samba	Samba	3.0.0	All	All	All
Application	Samba	Samba	3.0.1	All	All	All
Application	Samba	Samba	3.0.0	All	All	All
Application	Samba	Samba	3.0.1	All	All	All

cpe:2.3:a:samba:samba:3.0.0:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:3.0.1:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:3.0.0:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:3.0.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→