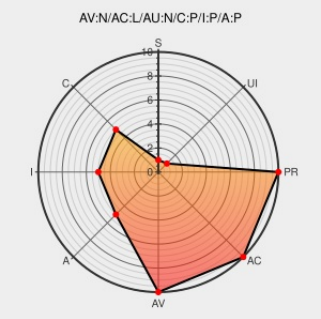
CVE-2005-3280

Published on: 10/23/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

CVE-2005-3280

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



Certain versions of Paros from Paros contain the following vulnerability:

Paros 3.2.5 uses a default password for the "sa" account in the underlying HSQLDB database and does not restrict access to the local machine, which allows remote attackers to gain privileges.

CVE-2005-3280 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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF paros-password-security-bypass(22557)
Secunia - Advisories - Gentoo update for paros	web.archive.org text/html	SECUNIA 18626
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060130 Re: [Full-disclosure] [GLSA 200601-15] Paros: Default administrator password
Gentoo Linux Documentation -- Paros: Default administrator password	www.gentoo.org text/html	GENTOO GLSA-200601-15
Paros HSQLDB Remote Authentication Bypass Vulnerability	Patch cve.report (archive) text/html	BID 15141
Secunia - Advisories - Paros hsqldb Exposure	Patch	SECUNIA 17089

of Database Content	Vendor Advisory web.archive.org text/html	
No Description Provided	Exploit Patch Vendor Advisory www.zone-h.com text/html	MISC www.zone-h.com/en/advisories/read/id=8286/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paros	Paros	3.2.5	All	All	All
Application	Paros	Paros	3.2.5	All	All	All

cpe:2.3:a:paros:paros:3.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:paros:paros:3.2.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→