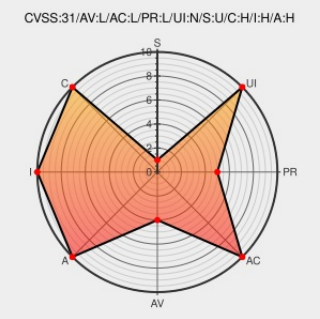
CVE-2014-7303

Published on: 01/27/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:50 PM UTC

CVE-2014-7303

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



Certain versions of Sgi Tempo from Hp contain the following vulnerability:

SGI Tempo, as used on SGI ICE-X systems, uses weak permissions for certain files, which allows local users to obtain password hashes and possibly other unspecified sensitive information by reading etc/dbdump.db.

CVE-2014-7303 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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
SGI Tempo Database Exposure ≈ Packet Storm	Mitigation Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/129467/SGI-Tempo-Database-Exposure.html

SGI Tempo System Database Exposure	Mitigation Third Party Advisory labs.f-secure.com text/html	MISC labs.f-secure.com/advisories/sgi-tempo-system-database-exposure/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Sgi Tempo	-	All	All	All
Application	Hp	Sgi Tempo	-	All	All	All

cpe:2.3:a:hp:sgi_tempo:-:*:*:*:*:*:*:*:

cpe:2.3:a:hp:sgi_tempo:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→