



CVE-2022-34320

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-34320
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-14 20:15:00 UTC
Updated	2023-11-07 03:48:00 UTC
Description	IBM CICS TX 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensi

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Cics Tx	11.1	All	All	All
Application	Ibm	Cics Tx	11.1	All	All	All

References

Reference	Source
Security Bulletin: IBM CICS TX Standard is vulnerable to attack because it uses weak cryptographic algorithms (CVE-2022-34320).	MISC
IBM X-Force Exchange	MISC
Security Bulletin: IBM CICS TX Advanced is vulnerable to attack because it uses weak cryptographic algorithms (CVE-2022-34320).	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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