CVE-2023-33850

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-33850
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-22 21:15:00 UTC
Updated	2023-08-28 19:51:00 UTC
Description	IBM GSKit-Crypto could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in tl

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Hp-ux	-	All	All	All
Operating System	Ibm	Aix	-	All	All	All
Application	Ibm	Cics Tx	10.1	All	All	All
Application	Ibm	Cics Tx	11.1	All	All	All
Application	Ibm	Cics Tx	11.1	All	All	All
Application	Ibm	Txseries For Multiplatform	8.1	All	All	All
Application	Ibm	Txseries For Multiplatform	8.2	All	All	All
Application	Ibm	Txseries For Multiplatform	9.1	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference	Source
Security Bulletin: "Timing Oracle in RSA Decryption" issue may affect GSKit shipped with IBM CICS TX Advanced	MISC
Security Bulletin: Timing Oracle in RSA Decryption vulnerability might affect GSKit supplied with IBM TXSeries for Multiplatforms.	MISC
Security Bulletin: "Timing Oracle in RSA Decryption " issue may affect GSKit shipped with IBM CICS TX Standard	MISC
IBM X-Force Exchange	MISC

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 20372 IBM DB2 information disclosure Vulnerability (7047481)
- 330167 IBM AIX Java Multiple Vulnerabilities (java_feb2024_advisory)
- 379387 IBM Java Software Development Kit (SDK) Security Vulnerability (7116432)
- 379431 IBM WebSphere Application ServerJava SDK Vulnerability (7058356)
- 755832 SUSE Enterprise Linux Security Update for java-1_8_0-ibm (SUSE-SU-2024:0605-1)
- 755835 SUSE Enterprise Linux Security Update for java-1_8_0-ibm (SUSE-SU-2024:0619-1)