CVE-2023-32342

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-32342
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-30 22:15:00 UTC
Updated	2023-06-06 18:18:00 UTC
Description	IBM GSKit could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in the RSA

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Http Server	All	All	All	All

References

Reference	Source	Link	Tags
IBM X-Force Exchange	MISC	exchange.xforce.ibmcloud.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

20382 IBM DB2 Information Disclosure Vulnerability (7066501)

378532 IBM Hypertext Transfer Protocol (HTTP) Server Information Disclosure Vulnerability (6998037)