CVE-2019-10202

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

Summary

CVE	CVE-2019-10202
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-01 15:15:00 UTC
Updated	2023-02-12 23:33:00 UTC
Description	A series of deserialization vulnerabilities have been discovered in Codehaus 1.9.x implemented in EAP 7. This CVE fixes C

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.2.0	All	All	All

References

Reference	Sou
Pony Mail!	MIS
Pony Mail!	MIS
Pony Mail!	MLI
Pony Mail!	MLI
Pony Mail!	MLI
Pony Mail!	MLI

Pony Mail!	MISC
Pony Mail!	MISC
Pony Mail!	MISC
Pony Mail!	MLIS
Pony Mail!	MISC
Pony Mail!	MLIS
1731271 – (CVE-2019-10202) CVE-2019-10202 codehaus: incomplete fix for unsafe deserialization in jackson-databind vulnerabilities	CON
Pony Mail!	MLIS
Pony Mail!	MISC
Pony Mail!	MLIS
Pony Mail!	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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