CVE-2017-1465

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

Summary

CVE	CVE-2017-1465
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-07 15:29:00 UTC
Updated	2017-12-19 15:11:00 UTC
Description	IBM TRIRIGA 3.2, 3.3, 3.4, and 3.5 could allow a remote attacker to hijack the clicking action of the victim. By persuading a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Tririga Application Platform	3.3.0.0	All	All	All
Application	Ibm	Tririga Application Platform	3.3.0.1	All	All	All
Application	Ibm	Tririga Application Platform	3.3.0.2	All	All	All
Application	Ibm	Tririga Application Platform	3.3.1.0	All	All	All
Application	Ibm	Tririga Application Platform	3.3.1.1	All	All	All
Application	Ibm	Tririga Application Platform	3.3.1.2	All	All	All
Application	Ibm	Tririga Application Platform	3.3.1.3	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.0	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.1	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.2	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.3	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.4	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.5	All	All	All
Application	Ibm	Tririga Application Platform	3.4.0.0	All	All	All
Application	Ibm	Tririga Application Platform	3.4.0.1	All	All	All
Application	Ibm	Tririga Application Platform	3.4.1.0	All	All	All
Application	Ibm	Tririga Application Platform	3.4.1.1	All	All	All

Application	Ibm	Tririga Application Platform	3.4.1.2	All	All	All
Application	Ibm	Tririga Application Platform	3.4.1.3	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.0	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.1	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.2	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.3	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.4	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.5	All	All	All
Application	Ibm	Tririga Application Platform	3.5.0.0	All	All	All
Application	Ibm	Tririga Application Platform	3.5.0.1	All	All	All
Application	Ibm	Tririga Application Platform	3.5.0.2	All	All	All
Application	Ibm	Tririga Application Platform	3.5.1	All	All	All
Application	Ibm	Tririga Application Platform	3.5.1.1	All	All	All
Application	Ibm	Tririga Application Platform	3.5.1.2	All	All	All
Application	Ibm	Tririga Application Platform	3.5.1.3	All	All	All
Application	Ibm	Tririga Application Platform	3.5.2	All	All	All
Application	Ibm	Tririga Application Platform	3.5.2.1	All	All	All
Application	Ibm	Tririga Application Platform	3.5.2.2	All	All	All
Application	Ibm	Tririga Application Platform	3.5.2.3	All	All	All
Application	Ibm	Tririga Application Platform	3.5.3	All	All	All
Application	Ibm	Tririga Application Platform	3.3.0.0	All	All	All
Application	Ibm	Tririga Application Platform	3.3.0.1	All	All	All
Application	Ibm	Tririga Application Platform	3.3.0.2	All	All	All
Application	Ibm	Tririga Application Platform	3.3.1.0	All	All	All
Application	Ibm	Tririga Application Platform	3.3.1.1	All	All	All
Application	Ibm	Tririga Application Platform	3.3.1.2	All	All	All
Application	Ibm	Tririga Application Platform	3.3.1.3	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.0	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.1	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.2	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.3	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.4	All	All	All
Application	Ibm	Tririga Application Platform	3.3.2.5	All	All	All
Application	Ibm	Tririga Application Platform	3.4.0.0	All	All	All
Application	Ibm	Tririga Application Platform	3.4.0.1	All	All	All

Application	Ibm	Tririga Application Platform	3.4.1.0	All	All	All
Application	Ibm	Tririga Application Platform	3.4.1.1	All	All	All
Application	Ibm	Tririga Application Platform	3.4.1.2	All	All	All
Application	Ibm	Tririga Application Platform	3.4.1.3	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.0	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.1	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.2	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.3	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.4	All	All	All
Application	Ibm	Tririga Application Platform	3.4.2.5	All	All	All
Application	Ibm	Tririga Application Platform	3.5.0.0	All	All	All
Application	Ibm	Tririga Application Platform	3.5.0.1	All	All	All
Application	Ibm	Tririga Application Platform	3.5.0.2	All	All	All
Application	Ibm	Tririga Application Platform	3.5.1	All	All	All
Application	Ibm	Tririga Application Platform	3.5.1.1	All	All	All
Application	Ibm	Tririga Application Platform	3.5.1.2	All	All	All
Application	Ibm	Tririga Application Platform	3.5.1.3	All	All	All
Application	Ibm	Tririga Application Platform	3.5.2	All	All	All
Application	Ibm	Tririga Application Platform	3.5.2.1	All	All	All
Application	Ibm	Tririga Application Platform	3.5.2.2	All	All	All
Application	Ibm	Tririga Application Platform	3.5.2.3	All	All	All
Application	Ibm	Tririga Application Platform	3.5.3	All	All	All

References

Reference	Source	Link
Security Bulletin: IBM TRIRIGA default login page has no defenses against clickjacking (CVE-2017-1465)	CONFIRM	www.ibm.com
IBM X-Force Exchange	MISC	exchange.xforce.ibm
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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