# CVE-2017-1171

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2017-1171 |
| **State** | PUBLIC |
| **Assigner** | psirt@us.ibm.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2017-03-31 18:59:00 UTC |
| **Updated** | 2019-10-03 00:03:00 UTC |
| **Description** | The IBM TRIRIGA Application Platform 3.3, 3,4, and 3,5 contain a vulnerability that could allow an authenticated user to exe |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## 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 | 3.3.0.0 | 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 |

## References

| Reference | Source | Link |
|---|---|---|
| Security Bulletin: IBM TRIRIGA Application Platform Privilege Escalation (CVE-2017-1171) | CONFIRM | www.ibm.com |
| IBM TRIRIGA Application Platform CVE-2017-1171 Unspecified Remote Privilege Escalation Vulnerability | BID | www.securityfocus.c |
| 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.