



CVE-2021-29749

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-29749 |
| State | PUBLIC |
| Assigner | psirt@us.ibm.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-07-15 16:15:00 UTC |
| Updated | 2021-07-31 01:17:00 UTC |
| Description | IBM Secure External Authentication Server 6.0.2 and IBM Secure Proxy 6.0.2 is vulnerable to server-side request forgery (S |

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------------------------------------|---------|--------|---------|----------|
| Application | ibm | Secure External Authentication Server | 6.0.2 | All | All | All |
| Application | ibm | Secure Proxy | 6.0.2 | All | All | All |

References

| Reference | Source | Link |
|--|---------|---|
| Security Bulletin: Multiple Vulnerabilities were detected in IBM Secure External Authentication Server | CONFIRM | www.ibm.com |
| Security Bulletin: Unrestricted document type definition vulnerability affects IBM Sterling Secure Proxy | CONFIRM | www.ibm.com |
| IBM X-Force Exchange | XF | exchange.xforce.ibmcloud.com |
| 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.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)