



CVE-2018-11068

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-11068 |
| State | PUBLIC |
| Assigner | security_alert@emc.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-09-11 19:29:00 UTC |
| Updated | 2021-12-15 19:05:00 UTC |
| Description | RSA BSAFE SSL-J versions prior to 6.2.4 contain a Heap Inspection vulnerability that could allow an attacker with physical |

Risk And Classification

Problem Types: CWE-459

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|-----------------|---------|--------|---------|----------|
| Application | Dell | Bsafe Ssl-j | All | All | All | All |
| Application | Emc | Rsa Bsafe Ssl-j | All | All | All | All |
| Application | Emc | Rsa Bsafe Ssl-j | All | All | All | All |

References

| Reference | Source |
|---|--------|
| RSA BSAFE SSL-J Crypto Timing and Memory Access Errors Let Remote or Physically Local Users Obtain Keys - SecurityTracker | SECTR |
| Full Disclosure: DSA-2018-150:RSA BSAFE® SSL-J Multiple Vulnerabilities | FULLDI |
| CVE Program record | CVE.OP |
| NVD vulnerability detail | NVD |

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](#).

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