



CVE-2021-39270

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

Summary

CVE	CVE-2021-39270
State	PUBLIC
Assigner	responsible-disclosure@pingidentity.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-18 19:15:00 UTC
Updated	2023-11-07 03:37:00 UTC
Description	In Ping Identity RSA SecurID Integration Kit before 3.2, user impersonation can occur.

Risk And Classification

Problem Types: CWE-346

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pingidentity	Rsa Securid Integration Kit	All	All	All	All

References

Reference	Source	Link	Tags
Download PingFederate Ping Identity		www.pingidentity.com	
docs.pingidentity.com/bundle/integrations/page/yqq1563995045546.html		docs.pingidentity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Ping Identity credits Lockheed Martin Corporation for their responsible disclosure.

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

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