



CVE-2021-41770

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

Summary

CVE	CVE-2021-41770
State	PUBLIC
Assigner	responsible-disclosure@pingidentity.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-07 07:15:00 UTC
Updated	2023-11-07 03:39:00 UTC
Description	Ping Identity PingFederate before 10.3.1 mishandles pre-parsing validation, leading to an XXE attack that can achieve XML

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pingidentity	Pingfederate	All	All	All	All

References

Reference	Source	Link	Tags
Download PingFederate Ping Identity		www.pingidentity.com	
docs.pingidentity.com/bundle/pingfederate-103/page/ruz1628492711606.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 An Trinh of Calif. for their responsible disclosure.

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](#)