



CVE-2018-6186

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

Summary

CVE	CVE-2018-6186
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-01 14:29:00 UTC
Updated	2018-03-03 02:29:00 UTC
Description	Citrix NetScaler VPX through NS12.0 53.13.nc allows an SSRF attack via the /rapi/read_url URI by an authenticated attack

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Netscaler	12.0	All	All	All
Application	Citrix	Netscaler	12.0	All	All	All

References

Reference

- [Citrix NetScaler Application Delivery Controller and NetScaler Gateway Multiple Security Updates](#)
- [Privilege escalation on Citrix NetScaler VPX through SSRF vulnerability · GitHub](#)
- [Citrix NetScaler VPX CVE-2018-6186 Privilege Escalation Vulnerability](#)
- [Citrix NetScaler ADC and NetScaler Gateway Multiple Bugs Let Remote Users Download Files, Traverse the Directory, Conduct Cross-Site S](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)