



CVE-2007-3679

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

Summary

CVE	CVE-2007-3679
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-07-25 17:30:00 UTC
Updated	2018-10-15 21:29:00 UTC
Description	The Citrix EPA ActiveX control (aka the "endpoint checking control" or CCAOControl Object) before 4.5.0.0 in npCtxCAO.dll

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Access Gateway	All	hf1	advanced	All
Application	Citrix	Access Gateway	All	All	standard	All

References

Reference
24975
37845
CTX113815 - Vulnerabilities in Access Gateway Standard and Advanced Editions clients could result in arbitrary code execution - Citrix Knowledge Center
Citrix EPA ActiveX Control Design Flaw - CXSecurity.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
About Secunia Research Flexera
IBM X-Force Exchange
Citrix EPA ActiveX Control Design Flaw
CTX114028 - Hotfix AG2000_v455 Rev B - Access Gateway Standard Edition 4.5 - Citrix Knowledge Center
SecurityFocus
symantec.com has moved to broadcom.com
CVE Program record

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](#).

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

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