



CVE-2011-3007

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2011-3007
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-08-10 20:55:00 UTC
Updated	2017-08-29 01:29:00 UTC
Description	The myCIOScn ActiveX control (myCIOScn.dll) in McAfee SaaS Endpoint Protection 5.2.1 and earlier allows remote attacks

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	McAfee	SaaS Endpoint Protection	All	All	All	All

References

Reference	Source	Li
IBM X-Force Exchange	XF	e>
TippingPoint DVLabs	MISC	dV
McAfee KnowledgeBase - McAfee Security Bulletin - McAfee SaaS Endpoint Protection update fixes multiple ActiveX issues	CONFIRM	kc
74513	OSVDB	os
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nV

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](#).

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

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