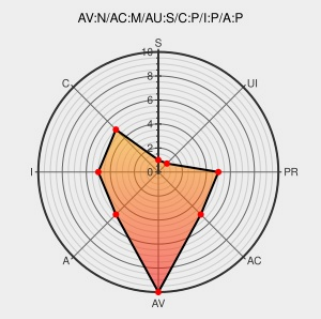
CVE-2007-3462

Published on: 06/27/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:34 PM UTC

CVE-2007-3462

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Safe At Office 500 Utm from Sofaware contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in Check Point SofaWare Safe@Office, with firmware before Embedded NGX 7.0.45 GA, allows remote attackers to execute commands as arbitrary users, and disable firewalling of the protected network.

CVE-2007-3462 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Calyptix Your Simple and Powerful Network Security Solution	labs.calyptix.com text/plain	MISC labs.calyptix.com/CX-2007-04.txt
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2007-2364
Check Point Safe@Office Input Validation Hole Permits Cross-Site Request Forgery Attacks - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1018317
Calyptix Security Advisory CX-2007-04: Cross-Site Request Forgery Against Check Point (Safe@Office)	Patch labs.calyptix.com text/html	MISC labs.calyptix.com/CX-2007-04.php
Check Point Products Cross-Site Request Forgery Vulnerability - Advisories - Secunia	web.archive.org text/html	SECUNIA 25822

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF safeatoffice-unspecified-csrf(35093)
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 37644
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20070626 Calyptix Security Advisory CX-2007-04 - Cross-Site Request Forgery Attack Against Check Point Safe@Office Device
SofaWare Technologies - Security Services	www.sofaware.com text/html	MISC www.sofaware.com/supportDownloads.aspx?boneId=182
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF safeatoffice-admin-password-modification(35094)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Sofaware	Safe At Office 500 Utm	embedded_ngx_7.0.39_ga	All	All	All
Hardware	Sofaware	Safe At Office 500 Utm	embedded_ngx_7.0.39_ga	All	All	All

cpe:2.3:h:sofaware:safe_at_office_500_utm:embedded_ngx_7.0.39_ga:*:*:*:*:*:*:*:

cpe:2.3:h:sofaware:safe_at_office_500_utm:embedded_ngx_7.0.39_ga:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→