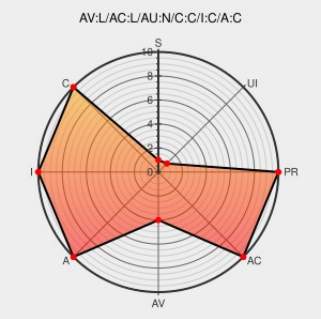
CVE-2006-0858

Published on: 02/23/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:06 PM UTC

CVE-2006-0858

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



Certain versions of Safe N Sec Personal Anti-spyware from Starforce contain the following vulnerability:

Unquoted Windows search path vulnerability in (1) snsmcon.exe, (2) the autostartup mechanism, and (3) an unspecified installation component in StarForce Safe'n'Sec Personal + Anti-Spyware 2.0 and earlier, and possibly other StarForce Safe'n'Sec products, might allow local users to gain privileges via a malicious "program" file in the C: folder.

CVE-2006-0858 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Safe'n'Sec Path Specification Local Privilege Escalation Vulnerabilities	cve.report (archive) text/html	BID 16762
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060219 [TZO-062006] Safe'nVulnerable
Sec Dev - Research and Development	web.archive.org text/html Inactive Link Not Archived	MISC secdev.zoller.lu/research/safnsec.htm

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Starforce	Safe N Sec Personal Anti-spyware	All	All	All	All
Application	Starforce	Safe N Sec Personal Anti-spyware	All	All	All	All

cpe:2.3:a:starforce:safe_n_sec_personal_+_anti-spyware:*:*:*:*:*:*:*:*:

cpe:2.3:a:starforce:safe_n_sec_personal_\+_anti-spyware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→