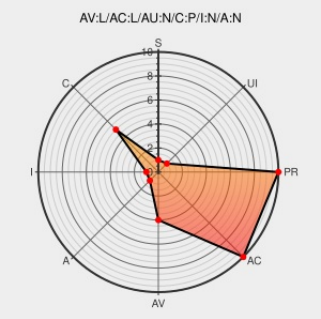
CVE-2005-1682

Published on: 05/20/2005 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1682

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



Certain versions of Solstice Internet Mail Server from Solstice contain the following vulnerability:

** DISPUTED ** JavaMail API, as used by Solstice Internet Mail Server POP3 2.0, does not properly validate the message number in the MimeMessage constructor in javax.mail.internet.InternetHeaders, which allows remote authenticated users to read other users' e-mail messages by modifying the msgno parameter. NOTE: Sun disputes this issue, stating "The report makes references to source code and files that do not exist in the mentioned products."

CVE-2005-1682 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
'JavaMail Information Disclosure (msgno)' - MARC	marc.info, text/html	BUGTRAQ 20050519 JavaMail Information Disclosure (msgno)
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory, www.vupen.com, text/html	VUPEN ADV-2005-0574

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Solstice	Solstice Internet Mail Server	pop3_2.0	All	All	All
Application	Solstice	Solstice Internet Mail Server	pop3_2.0	All	All	All

cpe:2.3:a:solstice:solstice_internet_mail_server:pop3_2.0:*:*:*:*:*:*:*:

cpe:2.3:a:solstice:solstice_internet_mail_server:pop3_2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→