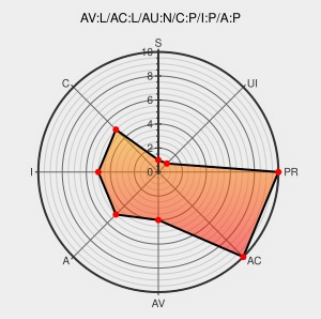
CVE-2005-2071

Published on: 06/29/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2071

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



Certain versions of Solaris from Sun contain the following vulnerability:

traceroute in Sun Solaris 10 on x86 systems allows local users to execute arbitrary code with PRIV_NET_RAWACCESS privileges via (1) a large number of -g arguments or (2) a malformed -s argument with a trailing . (dot).

CVE-2005-2071 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
SecurityTracker.com Archives - Sun Solaris traceroute(1M) Buffer Overflow in Processing '-g' Parameters Lets Local Users Gain Elevated Privileges	securitytracker.com, text/html	SECTRACK 1015261
No Description Provided	marc.info, text/html	BUGTRAQ 20050624 Re: Solaris 10 /usr/sbin/traceroute vulnerabilities
Sun Solaris Traceroute Multiple Local Buffer Overflow Vulnerabilities	Exploit, cve.report (archive), text/html	BID 14049
#102060: Security Vulnerabilities in the traceroute(1M) Utility may Allow Elevated Privileges	web.archive.org, text/html, Inactive Link, Not Archived	SUNALERT 102060
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory, www.vupen.com	VUPEN ADV-2005-2564

	text/html	
'Solaris 10 /usr/sbin/traceroute vulnerabilities' - MARC	marc.info text/html	BUGTRAQ 20050624 Solaris 10 /usr/sbin/traceroute vulnerabilities
Secunia - Advisories - Sun Solaris traceroute Commandline Buffer Overflow Vulnerability	Vendor Advisory web.archive.org text/html	SECUNIA 17708
No Description Provided	marc.info text/html	BUGTRAQ 20050624 Re: [Full-disclosure] Solaris 10 /usr/sbin/traceroute vulnerabilities

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
Operating System	Sun	Solaris	10.0	All	sparc	All
Operating System	Sun	Solaris	10.0	All	sparc	All

cpe:2.3:o:sun:solaris:10.0:*:sparc:*:*:*:*:*:

cpe:2.3:o:sun:solaris:10.0:*:sparc:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→