



CVE-2004-2012

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2012

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Netbsd](#) from [Netbsd](#) contain the following vulnerability:

The `systrace_exit` function in the `systrace` utility for NetBSD-current and 2.0 before April 16, 2004, and certain FreeBSD ports, does not verify the owner of the `/dev/systrace` connection before setting `euid` to 0, which allows local users to gain root privileges.

CVE-2004-2012 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

'Advisory 04/2004: Net(Free)BSD Systrace local root vulnerability' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20040510 Advisory 04/2004: Net\(Free\)BSD Systrace local root vulnerability](#)

Secunia - Advisories - NetBSD Systrace Privilege Escalation Vulnerability

[web.archive.org](#)
[text/html](#)

[SECUNIA 11585](#)

NetBSD/FreeBSD Port Systrace Exit Routine Access Validation Privilege Escalation Vulnerability

[Exploit](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 10320](#)

[ftp.NetBSD.org](#)
[text/plain](#)

[NETBSD NetBSD-SA2004-007](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF systrace-gain-privileges\(16110\)](#)

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	Netbsd	Netbsd	2.0	All	All	All
Operating System	Netbsd	Netbsd	2.0	All	All	All
Application	Niels	Provos Systrace	1.1	All	All	All
Application	Niels	Provos Systrace	1.2	All	All	All
Application	Niels	Provos Systrace	1.3	All	All	All
Application	Niels	Provos Systrace	1.4	All	All	All
Application	Niels	Provos Systrace	1.5	All	All	All
Application	Niels	Provos Systrace	1.1	All	All	All
Application	Niels	Provos Systrace	1.2	All	All	All
Application	Niels	Provos Systrace	1.3	All	All	All
Application	Niels	Provos Systrace	1.4	All	All	All
Application	Niels	Provos Systrace	1.5	All	All	All
Application	Vladimir Kotal	Systrace Port For Freebsd	2004-03-09	All	All	All
Application	Vladimir Kotal	Systrace Port For Freebsd	2004-06-02	All	All	All
Application	Vladimir Kotal	Systrace Port For Freebsd	2004-03-09	All	All	All
Application	Vladimir Kotal	Systrace Port For Freebsd	2004-06-02	All	All	All
cpe:2.3:o:netbsd:netbsd:2.0:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:2.0:*:*:*:*:*:						
cpe:2.3:a:niels:provos_systrace:1.1:*:*:*:*:*:						
cpe:2.3:a:niels:provos_systrace:1.2:*:*:*:*:*:						
cpe:2.3:a:niels:provos_systrace:1.3:*:*:*:*:*:						
cpe:2.3:a:niels:provos_systrace:1.4:*:*:*:*:*:						
cpe:2.3:a:niels:provos_systrace:1.5:*:*:*:*:*:						
cpe:2.3:a:niels:provos_systrace:1.1:*:*:*:*:*:						
cpe:2.3:a:niels:provos_systrace:1.2:*:*:*:*:*:						

cpe:2.3:a:niels:provos_systrace:1.2:*****:
cpe:2.3:a:niels:provos_systrace:1.3:*****:
cpe:2.3:a:niels:provos_systrace:1.4:*****:
cpe:2.3:a:niels:provos_systrace:1.5:*****:
cpe:2.3:a:vladimir_kotal:systrace_port_for_freebsd:2004-03-09:*****:
cpe:2.3:a:vladimir_kotal:systrace_port_for_freebsd:2004-06-02:*****:
cpe:2.3:a:vladimir_kotal:systrace_port_for_freebsd:2004-03-09:*****:
cpe:2.3:a:vladimir_kotal:systrace_port_for_freebsd:2004-06-02:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)