



# CVE-1999-0524

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-1999-0524
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	1997-08-01 04:00:00 UTC
<b>Updated</b>	2022-11-14 19:33:00 UTC
<b>Description</b>	ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.

## Risk And Classification

**Problem Types:** CWE-200 | NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	-	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	-	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Ios</a>	All	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Ios</a>	-	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Ios</a>	All	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">Hp-ux</a>	All	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">Hp-ux</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">Hp-ux</a>	All	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">Tru64</a>	All	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">Tru64</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">Tru64</a>	All	All	All	All
Operating System	<a href="#">Ibm</a>	<a href="#">Aix</a>	All	All	All	All

Operating System	<a href="#">Ibm</a>	<a href="#">Aix</a>	-	All	All	All
Operating System	<a href="#">Ibm</a>	<a href="#">Aix</a>	All	All	All	All
Operating System	<a href="#">Ibm</a>	<a href="#">Os2</a>	All	All	All	All
Operating System	<a href="#">Ibm</a>	<a href="#">Os2</a>	-	All	All	All
Operating System	<a href="#">Ibm</a>	<a href="#">Os2</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">All Windows</a>	abstract_cpe	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">All Windows</a>	abstract_cpe	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Netware</a>	All	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Netware</a>	-	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Netware</a>	All	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	-	All	All	All
Operating System	<a href="#">Santa Cruz Operation</a>	<a href="#">Sco Unix</a>	All	All	All	All
Operating System	<a href="#">Santa Cruz Operation</a>	<a href="#">Sco Unix</a>	All	All	All	All
Operating System	<a href="#">Sco</a>	<a href="#">Sco Unix</a>	-	All	All	All
Operating System	<a href="#">Sgi</a>	<a href="#">Irix</a>	-	All	All	All
Operating System	<a href="#">Windriver</a>	<a href="#">Bsdos</a>	All	All	All	All
Operating System	<a href="#">Windriver</a>	<a href="#">Bsdos</a>	-	All	All	All
Operating System	<a href="#">Windriver</a>	<a href="#">Bsdos</a>	All	All	All	All

## References

Reference	Source	Link
VMware Knowledge Base - View Document	MISC	<a href="#">kb.vmware.com</a>
IBM X-Force Exchange	XF	<a href="#">exchange.xforce.ibmcloud.com</a>
McAfee KnowledgeBase - McAfee Security Bulletin – Network Data Loss Prevention addresses 17 security issues	CONFIRM	<a href="#">kc.mcafee.com</a>
<a href="#">descriptions.securesscout.com/tc/11010</a>	MISC	<a href="#">descriptions.securesscout.com/tc/11010</a>
95	OSVDB	<a href="#">www.osvdb.org</a>
IBM X-Force Exchange	XF	<a href="#">exchange.xforce.ibmcloud.com</a>
<a href="#">descriptions.securesscout.com/tc/11011</a>	MISC	<a href="#">descriptions.securesscout.com/tc/11011</a>
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView	CONFIRM	<a href="#">kb.juniper.net</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

## Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-01-05	Joshua Bressers	Red Hat Enterprise Linux is configured by default to respond to all ICMP requests. Users ma

## Legacy QID Mappings

900101	CBL-Mariner Linux Security Update for kernel 5.10.52.1
900303	CBL-Mariner Linux Security Update for kernel 5.10.57.1
900321	CBL-Mariner Linux Security Update for kernel 5.10.60.1
901541	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6510-1)
902874	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3468)
906150	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3468-1)
906443	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6510-2)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)