



CVE-2009-1893

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

Summary

CVE	CVE-2009-1893
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-17 16:30:00 UTC
Updated	2023-02-13 01:17:00 UTC
Description	The configtest function in the Red Hat dhcpd init script for DHCP 3.0.1 in Red Hat Enterprise Linux (RHEL) 3 allows local users to execute arbitrary commands with root privileges by using a crafted DHCP request packet. This is due to the fact that the configtest function does not properly validate the user input before executing the command. The configtest function is used to test the configuration of the DHCP server. It is called by the dhcpd init script when the server is started. The configtest function takes a user input and executes the command specified by the user input. The user input is not properly validated before being executed, which allows local users to execute arbitrary commands with root privileges.

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	lsc	Dhcp	3.0.1	rc1	All	All
Application	lsc	Dhcp	3.0.1	rc10	All	All
Application	lsc	Dhcp	3.0.1	rc11	All	All
Application	lsc	Dhcp	3.0.1	rc12	All	All
Application	lsc	Dhcp	3.0.1	rc13	All	All
Application	lsc	Dhcp	3.0.1	rc14	All	All
Application	lsc	Dhcp	3.0.1	rc2	All	All
Application	lsc	Dhcp	3.0.1	rc5	All	All
Application	lsc	Dhcp	3.0.1	rc6	All	All
Application	lsc	Dhcp	3.0.1	rc7	All	All
Application	lsc	Dhcp	3.0.1	rc8	All	All
Application	lsc	Dhcp	3.0.1	rc9	All	All
Application	lsc	Dhcp	3.0.1	rc1	All	All
Application	lsc	Dhcp	3.0.1	rc10	All	All
Application	lsc	Dhcp	3.0.1	rc11	All	All
Application	lsc	Dhcp	3.0.1	rc12	All	All
Application	lsc	Dhcp	3.0.1	rc13	All	All

Application	Isc	Dhcp	3.0.1	rc14	All	All
Application	Isc	Dhcp	3.0.1	rc2	All	All
Application	Isc	Dhcp	3.0.1	rc5	All	All
Application	Isc	Dhcp	3.0.1	rc6	All	All
Application	Isc	Dhcp	3.0.1	rc7	All	All
Application	Isc	Dhcp	3.0.1	rc8	All	All
Application	Isc	Dhcp	3.0.1	rc9	All	All
Operating System	Redhat	Enterprise Linux	3.0	All	All	All
Operating System	Redhat	Enterprise Linux	3.0	All	as	All
Operating System	Redhat	Enterprise Linux	3.0	All	es	All
Operating System	Redhat	Enterprise Linux	3.0	All	ws	All
Operating System	Redhat	Enterprise Linux	3.0	All	All	All
Operating System	Redhat	Enterprise Linux	3.0	All	as	All
Operating System	Redhat	Enterprise Linux	3.0	All	es	All
Operating System	Redhat	Enterprise Linux	3.0	All	ws	All

References						
Reference				Source	Link	
Support				REDHAT	www.redh	
SecurityTracker.com Archives - Red Hat dhcpd init Script Symlink Flaw Lets Local Users Gain Elevated Privileges				SECTrack	securitytra	
CVE-2009-1893 - Red Hat Customer Portal				MISC	access.re	
IBM X-Force Exchange				XF	exchange	
510024 – (CVE-2009-1893) CVE-2009-1893 dhcp: insecure temporary file use in the dhcpd init script				CONFIRM	bugzilla.re	
Red Hat update for dhcp - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA	secunia.co	
Repository / Oval Repository				OVAL	oval.cisec	
ISC DHCP 'dhcpd -t' Command Insecure Temporary File Creation Vulnerability				BID	www.secu	
Red Hat Customer Portal				MISC	access.re	
Repository / Oval Repository				OVAL	oval.cisec	
CVE Program record				CVE.ORG	www.cve.o	
NVD vulnerability detail				NVD	nvd.nist.g	

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

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