CVE-2009-0692

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-0692
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-14 20:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Stack-based buffer overflow in the script_write_params method in client/dhclient.c in ISC DHCP dhclient 4.1 before 4.1.0p1

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Isc	Dhcp	2.0	All	All	All

Application	Isc	Dhcp	3.0	All	All	All
Application	Isc	Dhcp	3.1	All	All	All
Application	Isc	Dhcp	4.0	All	All	All
Application	Isc	Dhcp	4.1.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
The Slackware Linux Project: Slackware Security Advisories	af854a3
[security-announce] SUSE Security Announcement: dhcp-client (SUSE-SA:200	af854a3
[SECURITY] Fedora 10 Update: dhcp-4.0.0-37.fc10	af854a3
ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2009-010.txt.asc	af854a3
NetBSD update for ISC dhclient - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3
US-CERT Vulnerability Note VU#410676	af854a3
Gentoo Linux Documentation -- ISC DHCP: dhcpclient Remote execution of arbitrary code	af854a3
Red Hat update for dhcp - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3
| Internet Systems Consortium	af854a3
DHCP | Internet Systems Consortium	af854a3
Bug 507717 – CVE-2009-0692 dhclient: stack overflow leads to arbitrary code execution as root	af854a3
SUSE update for dhcp-client - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3
HP Insight Control Suite For Linux Multiple Vulnerabilities - Advisories - Community	af854a3
ISC DHCP "script_write_params()" Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3
ISC DHCP 'dhclient' 'script_write_params()' Stack Buffer Overflow Vulnerability	af854a3
SecurityTracker.com Archives - DHCP dhclient Stack Overflow in script_write_params() Lets Remote Users Execute Arbitrary Code	af854a3
Debian update for dhcp3 - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3
Support / Security / Advisories / / MDVSA-2009:151 | Mandriva	af854a3
itrc.hp.com/service/cki/docDisplay.do	af854a3
Ubuntu update for dhcp3 - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3
USN-803-1: dhcp vulnerability | Ubuntu	af854a3
Repository / Oval Repository	af854a3
Support	af854a3
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3
Gentoo update for dhcp - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3

Gentoo update for dhcp - Secunia Advisories - Vulnerability Information - Secunia.com	af854a
Debian update for dhcp3 - Secunia Advisories - Vulnerability Information - Secunia.com	af854a
[SECURITY] Fedora 11 Update: dhcp-4.1.0p1-4.fc11	af854a
www.osvdb.org/55819	af854a
Fedora update for dhcp - Secunia Advisories - Vulnerability Information - Secunia.com	af854a
Red Hat update for dhcp - Secunia Advisories - Vulnerability Information - Secunia.com	af854a
Fedora update for dhcp - Secunia.com	af854a
Debian -- Security Information -- DSA-1833-1 dhcp3	af854a
Repository / Oval Repository	af854a
Support	af854a
Slackware update for dhcp - Secunia Advisories - Vulnerability Information - Secunia.com	af854a
CVE Program record	CVE.O
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-07-16	Tomas Hoger	This issue affected the dhcp packages as shipped with Red Hat Enterprise Linux 3 and 4. Upda

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