CVE-2021-25217: A buffer overrun in lease file parsing code can be used to exploit a common vulnerability shared by dhcpd and dhclient

Updated on 26 May 2021 • 4 Minutes to read • Contributors

CVE: CVE-2021-25217 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25217)

Document version: 2.0

Posting date: 26 May 2021

Program impacted: ISC DHCP (https://www.isc.org/dhcp/). Due to shared code, multiple components are affected; please continue reading for details.

Versions affected: ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16, ISC DHCP 4.4.0 -> 4.4.2.
Other branches of ISC DHCP (i.e., releases in the 4.0.x series or lower and releases in the 4.3.x series) are beyond their End-of-Life (EOL) and no longer supported by ISC. From inspection it is clear that the defect is also present in releases from those series, but they have not been officially tested for the vulnerability.

Severity: High

Exploitable: Remotely

Description:

Program code used by the ISC DHCP package to read and parse stored leases has a defect that can be exploited by an attacker to cause one of several undesirable outcomes, depending on the component attacked and the way in which it was compiled.

Because of a discrepancy between the code which handles encapsulated option information in leases transmitted "on the wire" and the code which reads and parses lease information after it has been written to disk storage, it is potentially possible for an attacker to deliberately cause a situation where:

- `dhcpd` , while running in DHCPv4 or DHCPv6 mode, or
- `dhclient` , the ISC DHCP client implementation

will attempt to read a stored lease that contains option information which will trigger a bug in the option parsing code.

Impact:

The outcome of encountering the defect while reading a lease that will trigger it varies, according to:

- the component being affected (i.e., `dhclient` or `dhcpd`)
- whether the package was built as a 32-bit or 64-bit binary
- whether the compiler flag `-fstack-protection-strong` was used when compiling

In `dhclient` , ISC has not successfully reproduced the error on a 64-bit system. However, on a 32-bit system it is possible to cause `dhclient` to crash when reading an improper lease, which could cause network connectivity problems for an affected system due to the absence of a running DHCP client process.

In `dhcpd` , when run in DHCPv4 or DHCPv6 mode:

- if the `dhcpd` server binary was built for a 32-bit architecture AND the `-fstack-protection-strong` flag was specified to the compiler, `dhcpd` may exit while parsing a lease file containing an objectionable lease, resulting in lack of service to clients. Additionally, the offending lease and the lease immediately following it in the lease database may be improperly deleted.
- if the `dhcpd` server binary was built for a 64-bit architecture OR if the `-fstack-protection-strong` compiler flag was NOT specified, the crash will not occur, but it is possible for the offending lease and the lease which immediately followed it to be improperly deleted.

CVSS Scores:

Against `dhclient` , the ISC DHCP client: 7.4
Against `dhcpd` , the ISC DHCP server: 6.5

CVSS Vectors:

`dhclient` : CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C&version=3.1)

`dhcpd` : CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C&version=3.1)

For more information on the Common Vulnerability Scoring System and to obtain your specific environmental score, please visit: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C&version=3.1 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C&version=3.1).

Workarounds:

None known.

Active exploits:

We are not aware of any active exploits.

Solution:

Upgrade to the patched release most closely related to your current version of ISC DHCP:

- ISC DHCP 4.1-ESV-R16-P1
- ISC DHCP 4.4.2-P1

Acknowledgements:

ISC would like to thank Jon Franklin from Dell and Pawel Wieczorkiewicz from Amazon Web Services for (independently) reporting this vulnerability.

Document revision history:

1.0 Early Notification, 05 May 2021
1.1 Advance Security Notification, 19 May 2021
2.0 Public Disclosure, 26 May 2021

Do you still have questions? Questions regarding this advisory should go to security-officer@isc.org. *To report a new issue, please encrypt your message using security-officer@isc.org's PGP key, which can be found here: **https://www.isc.org/pgpkey/** (https://www.isc.org/pgpkey/). If you are unable to use encrypted email, you may also report new issues at: **https://www.isc.org/reportbug/** (https://www.isc.org/reportbug/).*

Note:

ISC patches only currently supported versions. When possible we indicate EOL versions affected. (For current information on which versions are actively supported, please see **https://www.isc.org/download/** (https://www.isc.org/download/).)

ISC Security Vulnerability Disclosure Policy:

Details of our current security advisory policy and practice can be found in the ISC Software Defect and Security Vulnerability Disclosure Policy at **https://kb.isc.org/docs/aa-00861** (https://kb.isc.org/docs/aa-00861).

The Knowledgebase article **https://kb.isc.org/docs/cve-2021-25217** (https://kb.isc.org/docs/cve-2021-25217) is the complete and official security advisory document.

Legal Disclaimer:

Internet Systems Consortium (ISC) is providing this notice on an "AS IS" basis. No warranty or guarantee of any kind is expressed in this notice and none should be implied. ISC expressly excludes and disclaims any warranties regarding this notice or materials referred to in this notice, including, without limitation, any implied warranty of merchantability, fitness for a particular purpose, absence of hidden defects, or of non-infringement. Your use or reliance on this notice or materials referred to in this notice is at your own risk. ISC may change this notice at any time. A stand-alone copy or paraphrase of the text of this document that omits the document URL is an uncontrolled copy. Uncontrolled copies may lack important information, be out of date, or contain factual errors.

Previous
CVE-2022-2928 An option refcount overflow exists in dhcpd

Next
CVE-2018-5733: A malicious client can overflow a reference counter in ISC dhcpd