Talos Vulnerability Report

TALOS-2020-1142

Systemd DHCP client denial-of-service vulnerability

APRIL 26, 2021

CVE NUMBER

CVE-2020-13529

Summary

An exploitable denial-of-service vulnerability exists in Systemd 245. A specially crafted DHCP FORCERENEW packet can cause a server running the DHCP client to be vulnerable to a DHCP ACK spoofing attack. An attacker can forge a pair of FORCERENEW and DCHP ACK packets to reconfigure the server.

Tested Versions

Canonical Ubuntu 20.04 LTS
Systemd 245

Product URLs

https://freedesktop.org/wiki/Software/systemd/

CVSSv3 Score

6.1 - CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H

CWE

CWE-290 - Authentication Bypass by Spoofing

Details

Systemd is a collection of utilities used in Linux systems to provide system management services. It runs as the first process and then starts the rest of the system services. It is meant as a replacement for sysvinit and has a range of different functionalities related to system management. It is used by default in some versions of Ubuntu.

A vulnerability exists in systemd's DHCP client which allows an attacker on the same network to reconfigure the specified target device by forging FORCERENEW and DHCP ACK packets. This vulnerability could then be used to misconfigure the device's network interface potentially resulting in a denial of service or possibly used in a man in the middle attack. This attack uses two weaknesses in systemd's DHCP implementation.

When systemd first initializes the DHCP client, it assigns a Transaction ID (xid) to be used for future transactions [1]. This allows systemd to filter out DHCP response packets which do not match the Transaction ID. This Transaction ID is sent to the broadcast MAC address per DHCP specification. It does not appear to change.

Systemd also implements RFC 3203, DHCP reconfigure extension [2]. This allows a DHCP server to send a FORCERENEW packet to the DHCP client to transition the client from the BOUND state to the RENEWING state [3]. However, systemd does not implement authentication on the FORCERENEW packet per RFC 3203 section 6.1 [4].

While the systemd DHCP client is in the RENEWING state, the attacker can now forge DHCP ACK packets using the previously noted Transaction ID to reconfigure the networking properties of the target device.

Systemd's DHCP client listens on port 68.

An attacker is able to reconfigure a target device running systemd's DHCP client by performing the following steps:

1. Listening for broadcast Transaction IDs over the network
2. Forge a FORCERENEW packet to the target device running systemd.
3. Forge a series of DHCP ACK packets with the Transaction ID and arbitrary settings directed to the systemd DHCP client.
4. The target device will use the DHCP ACK response and configure itself accordingly.
5. If this attack fails due to timing, the attacker can repeat steps 2-4.

[1] https://github.com/systemd/systemd/blob/master/src/libsystemd-network/sd-dhcp-client.c#L1375 [2] https://github.com/systemd/systemd/blob/master/src/libsystemd-network/sd-dhcp-client.c#L1444 [3] https://github.com/systemd/systemd/blob/master/src/libsystemd-network/sd-dhcp-client.c#L1836-L1839 [4] https://github.com/systemd/systemd/commit/615c1467c81411bf1d19fd7092e8995b5ebadc13

Timeline

2020-08-19 - Vendor Disclosure
2020-09-20 - Vendor acknowledged
2020-11-05 - 45 day follow up
2020-11-17 - 2nd follow up
2020-12-04 - Vendor advised issue planned for next release
2020-12-15 - Vendor advised issue will be treated as an RFE via a public issue
2021-03-22 - Final follow up with vendor
2021-04-26 - Public Release

CREDIT

Discovered by Mitchell Frank of Cisco Systems, Inc.