|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CSE ID | Vulners Website | Name | Description | Mitigation |
| https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A | <https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A> |  |  | Patch dnsmasq to latest; if unavailable, disable DNSSEC or disable vulnerable functionality. |
| https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A | <https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A> |  |  | Same — upgrade dnsmasq or disable affected features. |
| EDB-ID:42943 | <https://vulners.com/exploitdb/EDB-ID:42943> |  | Publically available exploit targeting CVE‑2017‑14493 (stack overflow via DHCPv6). | Patch dnsmasq to ≥ 2.78; restart service. |
| EDB-ID:42942 | <https://vulners.com/exploitdb/EDB-ID:42942> |  | Heap overflow in ICMPv6/Router Advertisement (CVE‑2017‑14492) . | Update dnsmasq to ≥ 2.78; disable IPv6 RA features if not used (enable-ra, ra-names, etc.). |
| EDB-ID:42941 | <https://vulners.com/exploitdb/EDB-ID:42941> |  | Heap buffer overflow in DNS response parsing (CVE‑2017‑14491) . | Patch dnsmasq ≥ 2.78; restrict dnsmasq to trusted networks and apply privilege separation. |
| CVE-2017-14493 | <https://nvd.nist.gov/vuln/detail/CVE-2017-14493> |  | Stack-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DHCPv6 request. | Update dnsmasq to a patched version  sudo apt update  sudo apt install --only-upgrade dnsmasq  Note: If your system does not require dnsmasq, consider **disabling or uninstalling** it to reduce the attack surface. |
| CVE-2017-14492 | <https://vulners.com/exploitdb/CVE-2017-14492> |  | Heap overflow in IPv6 RA handling potentially exploitable via malicious RA . | Update dnsmasq to ≥ 2.78; disable IPv6 RA features (ra-\* options). |
| CVE-2017-14491 | <https://vulners.com/exploitdb/CVE-2017-14491> |  | Heap buffer overflow in DNSSEC extract\_name() logic, permitting remote code execution . | Patch dnsmasq ≥ 2.78; limit exposure of the DNS service to trusted sources. |
| CVE-2020-25682 | <https://vulners.com/exploitdb/CVE-2020-25682> |  | DNSSEC heap overflow in sort\_rrset(), enabling possible arbitrary code execution . | Upgrade dnsmasq to ≥ 2.83 (or RHEL 8: dnsmasq 2.79-13.el8\_3.1+). Or disable DNSSEC entirely (--dnssec off). |
| CVE-2020-25681 | https://vulners.com/exploitdb/CVE-2020-25681 |  | DNS cache poisoning via hash weaknesses allowing forged responses (no DNSSEC) . | Upgrade to ≥ 2.83 or disable DNS cache (cache-size=0). |

|  |
| --- |
|  |