dnscrypt-proxy

CVE-2024-36587

dnscrypt-proxy - PrivEsc

Insecure permissions in DNSCrypt-proxy v2.0.0alpha9 to v2.1.5 allows non-privileged attackers to escalate privileges to root via overwriting the binary dnscrypt-proxy.

Vulnerability Categorisation

Vendor: DNSCrypt

Product: dnscrypt-proxy (open-source)

Vulnerability Type: Privilege escalation

Attack Type: Local

Impact: Code Execution & privilege escalation

Attack Vectors: Binary planting

Affected Component: dnscrypt-proxy/dnscrypt-proxy/main.go

Affected Versions: 2.0.0 alpha9 to latest (June 2024)

Sophistication: Low

Opperating Systems: Linux, openBSD, MacOS, and Windows (UAC bypass).

Zero-Day Exploitation

Exploited In Wild: Unknown

Notes: There have been no public accounts regarding exploitation occurring.

Vulnerability Attack Vector

If dnscrypt-proxy has been installed as a service via ./dnscrypt-proxy -service install following the dnscrypt-proxy's installation guide (DNScrypt, 2022) a non root user can overwrite the binary dnscrypt-proxy with a malicious payload which will then be executed as root next time the dnscrypt-proxy service restarts (e.g. after reboot).

On windows the attack works the same, except the user gains LocalSystem privileges, bypassing UAC.

Affected Components

```
./dnscrypt-proxy -service install
```

```
dnscrypt-proxy/dnscrypt-proxy/main.go
```

```
func (p *program) Start(_ service.Service) (err error)
```