CVE-2024-36586

AddGuardHome - PrivEsc

An issue in AdGuardHome v0.93 to latest allows unprivileged attackers to escalate privileges via overwriting the AdGuardHome binary.

Vulnerability Categorisation

Vendor: AddGuard
Vendor: AddGuardHome(open-source)
Vulnerability Type: Privilege escalation
Attack Type: Local
Impact: Code Execution & privilege escalation
Attack Vectors: Binary planting
Affected Component: AdGuardHome -s install
Affected Versions: v0.93 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

To exploit this vulnerability an attacker must overwrite the AdGuardHome binary, replacing it with the malicious payload. Next the attacker must either wait or induce a restart of the daemon process, which will then execute the malicious payload under the user LocalSystem (Windows) or Root (Linux). However, the AdGuardHome service must already be installed.

Affected Components

```
./AdGuardHome -s install
```

```
/internal/home/service.go
```

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