Tartu Ülikool
Arvutiteaduse instituut

CVE-2024-3273: D-Link seadmete käsusüst

Uurimistöö

Autor: Oliver Pikani

Juhendaja: Tarmo Oja

Tartu 2024

Sisukord

1 Taust

D-Link Network Attached Storage (NAS) ehk võrgumälu seade on arvutivõrku ühendatav kõvakettaga (või -ketastega) seade failide talletuseks ja ühiskasutuseks.[Dig]

Erinevalt tavalisest välisest kõvakettast, mis on liidestatud otse arvutiga, ühendub võrgumälu seade kohtvõrguga, võimaldades mitmel kasutajal või seadmel üheaegselt faile kasutada ja jagada. Võrgumälu seadmed on kasutusel nii kodu- kui ka ärilahendustes.[D-L]

Turvauuringuid koostav ettevõte *VulDB Coordination* avastas osadel D-Link võrgumälu seadmetel kriitilise turvanõrkuse (CVE-2024-3273), mis võimaldab pahatahtlikel kasutajatel teha üle võrgu käsusüste, käivitades pahatahtlikke programmikäske ohvri seadmes.[Sup]

2 Turvaauk

Eeltingimused

Käesolev turvanõrkus puudutab vaid teatud D-Link seadmeid, mille eluiga on juba läbi ning tootja on nende seadmete tarkvaralise ja riistvaralise toetamise lõpetanud [net].

Mõjutatud on järgmised mudelid:

- DNS-320L Version 1.11, Version 1.03.0904.2013, Version 1.01.0702.2013
- DNS-325 Version 1.01
- DNS-327L Version 1.09, Version 1.00.0409.2013
- DNS-340L Version 1.08

[net]

Antud turvanõrkus eeldab ka ühe teise nõrkuse samaaegset ärakasutamist. Nimelt muudab võrgumälu seadme eriti haavatavaks püsiprogrmmeeritud sisselogimissuvandite põhjustatud tagauks. [NISa]

Selleks tagaukseks on turvanõrkus (CVE-2024-3272), kus kasutajal on võimalik autentimisest

mööda pääseda kasutades vaikimisi kõigis mõjutatud seadmetes olevat "süsteemikasutajat" *messagebus* [Grea].

Selle Linux süsteemides vaikimisi oleva süsteemi deemon (*system daemon*) kasutajaga ei saa küll otseselt süsteemi sisse logida, kuid piisab osavalt meisterdatud HTTP päringust kindlasse otspunkti, et juba kahju teha [Sta]. Vaja on teada ka rünnatava seadme ip addressi.

Turvaaugu avaldumine

Turvanõrkus peitub võrgumälu seadme */cgi-bin/nas_ sharing.cgi* failis HTTP GET päringu töötlemisfunktsioonis [CVE].

Pahatahtlikul kasutajal on võimalik saata GET päring üle võrgu ohvri seadmesse andes parameetritena kaasa kasutajanimi "messagebus"ja parool jätta tühjaks. Käsusüst tuleb siin mängu system parameetrit kasutades, määrates parameetri väärtuseks soovitud programmikäsu. [net]

Käsk peidetakse base64 kodeeringuga ning lisatakse system parameetri väärtuseks. Hiljem dekodeerides avaldub pahatahtlik käsujupp mis käivitub shell käsuna rünnatavas seadmes. [net]

CVSS Baasskoor: 7.3 Kõrge

- **AV: N -** Nõrkus on ära kasutatav üle võrgu.
- **AC: L -** Rünnaku keerukus on madal, kuna rünnakuks vajalikud vahendid on lihtsasti kättesaadavad.
- **PR: N -** Rünnakuks ei ole vaja eraldi privileege.
- **UI: N -** Kasutaja interaktsioon ei ole vajalik.
- **S: U -** Puudutab vaid kindlaid mudeleid ja ei laiene üle teistele seadmetele.
- **C: L -** Konfidentsiaalsuse mõju on madal, kuna rünnak ei paljasta olulist konfidentsiaalset teavet.
- **I: L -** Terviklikkuse mõju on madal, kuna rünnak ei muuda oluliselt süsteemi andmeid ega konfiguratsiooni.
- **A: L -** käideldavuse mõju on madal, kuna rünnak ei põhjusta teenuste katkemist.

[NISb].

Näide turvanõrkust ärakasutavast koodist on lisatud Lisa 2 alla.

Turvaaugu põhjused

Turvanõrkuse CVE-2024-3273 põhjuseks on CWE-77 ehk käsusüst [NISb]. See tähendab, et ründaja saab sisestada pahatahtlikke käske, mida rünnatav süsteem seejärel täidab, kuna sisestatud käsku ei valideerita [CWE].

Kuna seadmete lähtekood pole avalik siis arvatavasti tuleks selle probleemi vältimiseks lisada päringutega tegelevasse meetodisse valideerimisfunktsioon. Näiteks võiks olla list lubatud süsteemi käskudest, et vältida suvalise käsu jooksutamist. [Med]

3 Mõju ja turvaaugu kõrvaldamine

Mõju varadele

Turvanõrkus rikub peamiselt järgmisi turvaeesmärke:

- Konfidentsiaalsus: Ründaja võib saada juurdepääsu konfidentsiaalsetele andmetele, nt isiklikud andmed või ärisaladused
- Privaatsus: Saades ligipääsu konfidentsiaalsetele andmetele võib see rikkuda kasutaja privaatsust.
- Terviklus: Ründajal on võimalik muuta andmeid ja süsteemi seadeid
- Usaldusväärsus: Haavatavate D-Link seadmete kasutajad võivad kaotada usalduse tootja vastu.

Turvaaugu parandamine

Antud turvanõrkus puudutab vaid seadmeid, mille eluiga on juba läbi, seega soovitab tootja seadmed asendada ning haavatavaid seadmeid mitte kasutada [Sup].

Kuna neid seadmeid enam ei toetata, siis ei saa need enam ka tarkvaralisi turvauuendusi, mis tähendab et turvaauku ära ei parandata [Sup].

Seega ainuke lahendus on turvaauguga toodete kasutamine lõpetada.

Turvaaaugu mõju leevendamine

Kui haavatava seadme asendamine pole võimalik, tuleks seade kindlasti eemaldada avalikust võrgust ning äärmisel juhul olla kasutuses vaid lokaalses kohtvõrgus olevatele seadmetele (tuleks paigaldada tulemüür väliste päringute blokkeerimiseks) [Sha].

Turvaaugu tegelik ärakasutatavus

Esialgse raporti kohaselt oli turvaaugu avastamise hetkel võrgus üle 92 000 seadme [net]. Hilisema uuringu kohaselt võis see number olla aga oluliselt väiksem, jäädes 5500 seadme kanti [Grea].

Sellest hoolimata on täna veel tõenäoliselt paljud vanad seadmed veel endiselt võrku ühendatud ja seeläbi haavatavad.

Avaldatud on mitmeid rünnaku kontseptsiooni tõendusi (PoC) ning tõenäoliselt kasutatakse turvaauku endiselt laialdaselt ära [NISb].

Näidis koodijupist millega on võimalik kõnealust nõrkust ära kasutada on Lisa 2 all.

Praeguseks hetkeks on avastatud vähemalt 146 juhtumit, kus on proovitud ära kasutada CVE-2024-3273 turvanõrkust [Greb].

Kasutatud allikad

[Cho] Chocapikk. Example of exploit code in Github. (07.04.2024). https://github.com/Chocapikk/CVE-2024-3273/blob/main/exploit.py.

[CVE] CVE. CVE Records. (04.04.2024). https://www.cve.org/CVERecord?id=CVE-2024-3273.

[CWE] CWE. CWE-77: Command Injection. (01.11.2007). https://cwe.mitre.org/data/definitions/77.html.

[D-L] D-Link. Network Attached Storage in a Nutshell. (2011). https://sharecenter.dlink.com/ShareCenter_NAS_101.

[Dig] Digigeenius. Võrgumälu: mis see on ja kas peaksid selle ostma? (31.03.2021). https://digi.geenius.ee/rubriik/uudis/kovakettaga-uhendatav-vorgumalu-mis-see-on-ja-kas-peaksid-selle-ostma/.

[Grea] GreyNoise. CVE-2024-3273: D-Link NAS RCE Exploited in the Wild. (08.04.2024). https://www.greynoise.io/blog/cve-2024-3273-d-link-nas-rce-exploited-in-the-wild.

[Greb] GreyNoise. D-Link NAS CVE-2024-3273 RCE attempts. (04.04.2024). https://viz.greynoise.io/tags/d-link-nas-cve-2024-3273-rce-attempt?days=30.

[Med] Medium. CWE-77: Improper Neutralization of Special Elements used in a Command. (21.10.2021). https://blog.shiftleft.io/cwe-77-bf222588a521.

[net] netsecfish. Command Injection and Backdoor Account in D-Link NAS Devices, Github. (26.04.2024). https://github.com/netsecfish/dlink?tab=readme-ov-file.

[NISa] NIST. CVE-2024-3272 Detail. (04.03.2024). https://nvd.nist.gov/vuln/detail/CVE-2024-3272.

[NISb] NIST. CVE-2024-3273 Detail. (04.03.2024). https://nvd.nist.gov/vuln/detail/CVE-2024-3273.

[Sha] ShadowServer. CRITICAL: Vulnerable HTTP Report. (25.04.2024). https://www.shadowserver.org/what-we-do/network-reporting/vulnerable-http-report/.

[Sta] StackExchange. The other users in Linux. (08.01.2014). https://unix.stackexchange.com/questions/108447/the-other-users-avahi-root-syslog-messagebus-nobody-ntp-rtkit-and-whoops.

[Sup] D-Link Support. D-Link security announcement. (04.04.2024). https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383.

Lisa 1 – Litsents

Mina, **Oliver Pikani**, annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud uurimistööd teemal **CVE-2024-3273: D-Link seadmete käsusüst** avalikult eksponeerida kuni aastani 2029, k.a.

Oliver Pikani

5. mai 2024. a.

Lisa 2 – Näidiskood

Koodijupp näitest kust kasutatakse ära antud turvanõrkust ning milliste parameetritega täpselt päring teha tuleks [Cho].

```
def execute_command(self, command: str = "id", verbose: bool = True) -> str:
        command_hex = ''.join(f'\\\\x{ord(c):02x}' for c in command)
        command_final = f"echo -e {command_hex}|sh".replace(' ', '\t')
        base64_cmd: str = base64.b64encode(command_final.encode()).decode()
        url: str = f"{self.base_url}/cgi-bin/nas_sharing.cgi"
        params: dict = {
            "user": "messagebus",
            "passwd": "",
            "cmd": "15",
            "system": base64_cmd,
        }
```

Joonis 1. HTTP GET päringu näide