Closed Issue created 7 months ago by Martin Kaesberger

netstat is vulnerable to escape sequence injection (busybox)

Hey there,

Alpine ships BusyBox with the `netstat` applet enabled. This is vulnerable to escape sequence injection when used from an VT compatible terminal. To exploit this vulnerability the PTR for a remote host must contain a escape sequence and the victim has to execute `netstat`. I've set up an example at `[elided]` with the PTR resolving to `\027[33\;46mlocalhost.`

```
$ dig -x [elided] @8.8.8.8

; <<>> DiG 9.16.25 <<>> -x [elided] @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59625
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;[elided]. IN PTR

;; ANSWER SECTION:
[elided]. 1 IN PTR \027[33\;46mlocalhost.

;; Query time: 55 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Apr 03 00:11:16 DST 2022
;; MSG SIZE  rcvd: 132
```

If you try to `ssh [elided]` and run `netstat -t` while trying to establish the connection from a different terminal, the second terminal will change the background and font color. Other escape sequences may lead to code execution.

Edited 7 months ago by Ariadne Conill

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Child items 0

No child items are currently assigned. Use child items to prioritize tasks that your team should complete in order to accomplish your goals!

Linked items 0

Martin Kaesberger @mkaesberger changed the description 7 months ago

Martin Kaesberger @mkaesberger · 7 months ago Author Contributor

Please remove all IP addresses before making the issue public.

Edited by Martin Kaesberger 7 months ago

Jakub Jirutka UA @jirutka added tag:security label 7 months ago

Jakub Jirutka UA @jirutka · 7 months ago Developer

/cc @ariadne

Kevin Daudt @kdaudt · 7 months ago Owner

Has this been reported to busybox?

Martin Kaesberger @mkaesberger · 7 months ago

Author Contributor

It's not reported to busybox because I couldn't validate if it is specific to Alpine or a general issue.

Kevin Daudt 💻 @kdaudt · 7 months ago

Owner

I can reproduce this on Archlinux with busybox, so this is not related to Alpine Linux

Edited by Kevin Daudt 7 months ago

Please register or sign in to reply

Kevin Daudt 💻 @kdaudt added triage:upstream-issue label 7 months ago

Ariadne Conill 🐰 @ariadne · 7 months ago

Developer

`nslookup` is also vulnerable. Real `nslookup` escapes the sequences.

Edited by Ariadne Conill 7 months ago

Martin Kaesberger @mkaesberger · 7 months ago

Author Contributor

`traceroute` was also affected.

Please register or sign in to reply

Ariadne Conill 🐰 @ariadne · 7 months ago

Developer

BusyBox has `printable_string()` in `libbb`, checking for the best way to sanitize the DNS results.

Ariadne Conill 🐰 @ariadne · 7 months ago

Developer

Affected branches: 3.12 through 3.15 + edge.

Kevin Daudt 💻 @kdaudt added edge v3.13 v3.14 v3.15 labels 7 months ago

Kevin Daudt 💻 @kdaudt added v3.12 label 7 months ago

Ariadne Conill 🐰 @ariadne · 7 months ago

Developer

Mitigation pending.

Edited by Ariadne Conill 7 months ago

Kevin Daudt 💻 @kdaudt changed milestone to %3.15.4 7 months ago

Ariadne Conill 🐰 @ariadne changed the description 7 months ago

Ariadne Conill 🐰 @ariadne · 7 months ago

Developer

Normally, I would say to keep the issue confidential, but given the low severity, and the unlikeliness for a speedy upstream ACK at this time, I am going to go ahead and declassify it.

We should backport the hotfix to all release branches though in the meantime.

Edited by Ariadne Conill 7 months ago

Ariadne Conill 🐰 @ariadne made the issue visible to everyone 7 months ago

Ariadne Conill 🐰 @ariadne · 7 months ago Developer

Use CVE-2022-28391 to reference this issue.

Natanael Copa @ncopa · 7 months ago Owner

- ☑ 3.15-stable `2745de7e`
- ☑ 3.14-stable `c45db46b`
- ☑ 3.13-stable `58bddeef`
- ☑ 3.12-stable `41c9e389`

Edited by Natanael Copa 7 months ago

⊖ Natanael Copa @ncopa closed 7 months ago

Please register or sign in to reply