HEARTBLEED
WHY YOU SHOULD CARE

C J SILVERIO

DEVOPS AT NPM

@CEEJBOT

WHAT'S HEARTBLEED?

SECURITY VULNERABILITY DISCLOSED APRIL 7 2/3RDS OF ALL SECURE SERVERS

OPENSSL THE SECURE 'S' IN HTTPS://

HEARTBEAT
A PULSE FROM A CLIENT TO A SERVER & BACK

ALICE ⇢ PING ⇢ BOB
ALICE ⇠ PONG ⇠ BOB

ALICE LIES:
"PONG IS 64K LETTERS."

BOB TRUSTS HER.
HE SENDS ALICE TOO MUCH DATA.

THAT DATA IS THE BLEED IN HEARTBLEED

WHAT LEAKED?

EVERYTHING.

» your passwords

» your cookies

» server's passwords

» server's identifying certificates

EVERYTHING LEAKED.
FROM 2/3RDS OF THE SERVERS
ON THE INTERNET.

HOW LONG DID THIS LEAK EXIST?

TWO YEARS.

EVERYTHING LEAKED FROM 2/3RDS OF THE SERVERS ON THE INTERNET FOR TWO YEARS.

everything's not fine

HOW DID THIS HAPPEN?

ROGUE AGENCY: THE NSA? INCOMPETENCE?

NOW WHAT?

CHANGE YOUR PASSWORDS

CHANGE YOUR PASSWORDS FOR EVERYTHING

YES, EVERYTHING

USE A PASSWORD MANAGER
1PASSWORD
HTTPS://GETVAU.LT

TOSS YOUR COOKIES

TURN ON 2-FACTOR AUTH

RECAP

HEARTBLEED IS AS BAD AS IT GETS.

CHANGE PASSWORDS
DELETE COOKIES
2-FACTOR AUTH

DONATE
TO IMPORTANT
OPEN-SOURCE PROJECTS

BUY YOUR OPERATIONS STAFF
A DRINK

CHANGE YOUR PASSWORDS