Managing Security in

THE NODE.JS PROJECT

With your host

@MYLESBORINS

OH HAI

MY NAME IS MYLES

I am gainfully employed by Google as a Developer Advocate

FOCUSING ON THE NODE.JS ECOSYSTEM AND GCP

Google Cloud Platform

The opinions expressed in this talk are solely my own

A GLOSSARY

MITRE

CWE

Common Weakness Enumeration

CVE

Common Vulnerabilities and Exposures

CNA

CVE Numbering Authority

CVSS

Common Vulnerability Scoring System

ZERO DAY

EMBARGO

TRIAGE

HACKERONE

WHAT KIND OF VULNERABILITIES WILL WE DISCUSS TODAY?

Vulnerabilities to the core Node.js platform

Vulnnerabilities in the Node.js

Ecosystem

Vulnerabiltiies in Node.js

Applications

WHAT TYPES OF THREATS ARE THERE TO NODE.JS CORE?

Buffer Overflow

Denial of Service

Data Exfiltration

Remote Code Execution

Hostname Spoofing

Vulnerabilities in Dependencies

LIFECYCLE OF A VULNERABILITY IN CORE

Researcher Reports Bug

Triaged in HackerOne

Communicated and Confirmed

Solution Identified

Security Release Made

Vulnerability Disclosed

HTTPS://NODEJS.ORG/EN/SECURITY/

HTTPS://HACKERONE.COM/NODEJS/

CVE-2017-14919

CWE-20 Improper input validation

BLOG POST

FIX

CVE-2018-7160

CWE-290 Authentication Bypass by Spoofing

CWE-350 Reliance on Reverse DNS Resolution for a Security-Critical Action

BLOG POST

CVE-2018-12115

CWE-787 Out-of-bounds Write

BLOG POST

E_TOO_MANY_VULNS

WHAT TYPES OF THREATS ARE THERE TO THE ECOSYSTEM AND APPLICATIONS?

Everything from before

Supply Chain Attacks

Weak Crypto

Poor Developer Experience

Malicious 3rd party code

Query Injection

NODESECROADMAP.FYI

ECOSYSTEM HACKERONE

A case study in supply chain attacks

EVENTSTREAM

NOV 20TH, 2018

Github Report

HOW DO YOU PROTECT YOURSELF?

Always use the latest version of a maintained Node.js release line

NPM AUDIT

Tools like Greenkeeper or Dependabot

AUDIT ALL DEPENDENCIES

STILL ALLOW FOR VELOCITY

VIA SANDBOXING

WHERE DO YOU RUN

YOUR CODE?

QUESTIONS?

THANK YOU

@MYLESBORINS