

When the supply chain hits a sour note



DATADOG

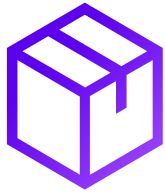


Kennedy Toomey

Application Security Researcher & Advocate @ Datadog

A terrible singer

Who's Afraid of Little Old Me?



npm package



Configured to
upgrade
automatically



Everything is
working great



New version is
released

Another One Bites the Dust

s1ngularity

August 26, 2025

- Targeted Nx
- Exploited vulnerable GitHub Actions workflow
- Added a credential-harvesting malware script
- Resulted in thousands of leaked secrets

debug/chalk

September 8, 2025

- Targeted npm maintainer known as Qix
- Gained access through a phishing email
- Malicious code functioned as a crypto stealer

Shai-Hulud

September 16, 2026

- Used unrotated tokens from s1ngularity
- Self-replicating worm
- Exfiltrated secrets and exposed private repos

Shai-Hulud 2.0

November 24, 2025

- Self-replicating worm
- backdoored 796 unique npm packages
- Leaked data from over 500 GitHub users



Another One Bites the Dust

s1ngularity

August 26, 2025

- Targeted Nx
- Exploited vulnerable GitHub Actions workflow
- Added a credential-harvesting malware script
- Resulted in thousands of leaked secrets

debug/chalk

September 8, 2025

- Targeted npm maintainer known as Qix
- Gained access through a phishing email
- Malicious code functioned as a crypto stealer

Shai-Hulud

September 16, 2026

- Used unrotated tokens from s1ngularity
- Self-replicating worm
- Exfiltrated secrets and exposed private repos

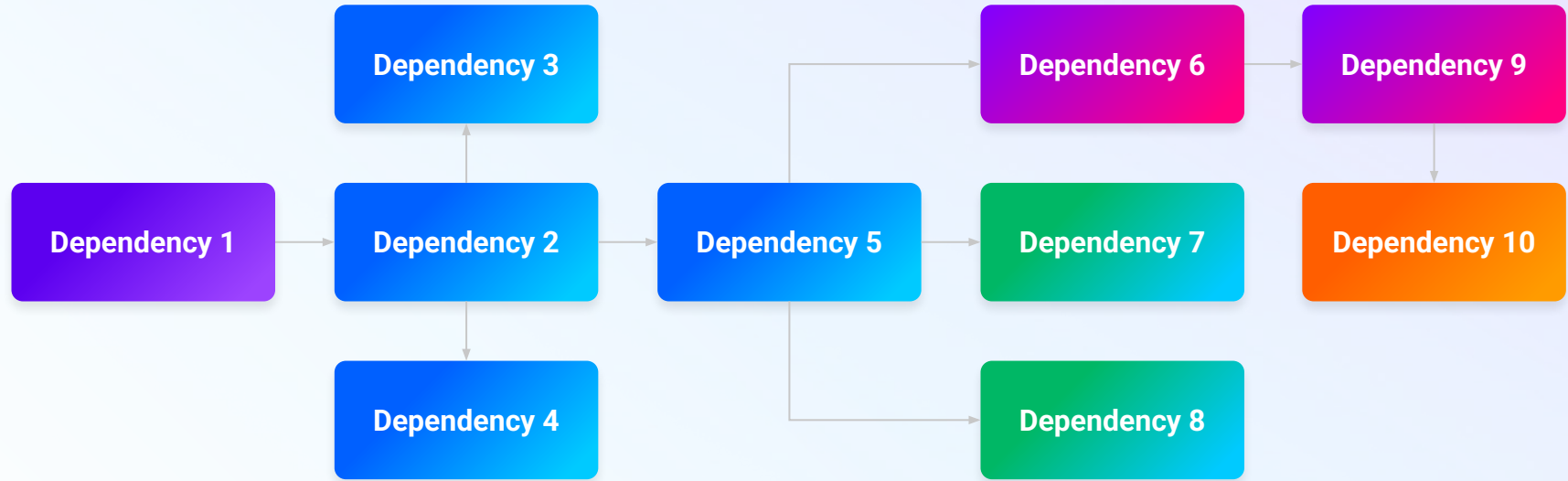
Shai-Hulud 2.0

November 24, 2025

- Self-replicating worm
- backdoored 796 unique npm packages
- Leaked data from over 500 GitHub users



Chain of Fools



Manic Monday

What happened?

- New information is being released

Are you affected?

- Does an SBOM exist? Is it current?

Stay organized

- Create a tracking sheet
- Assign clear responsibilities



Under Pressure

Leadership want
answers

Customers want to
know impact

New information keeps
being released

Come Together



Developers



DevOps



Security

You Can't Always Get What You Want



Least privilege and defense in depth

Goal: reduced attack surface



Proactive defenses

Ex. using FGAT, MFA, minimum package age

Hello (from the other side)



The Show Must Go On

Urgency

from security teams

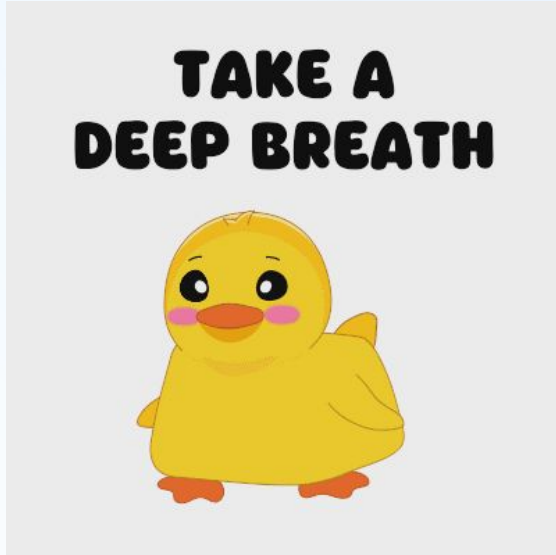


Urgency

from other teams



I'm Still Standing



Stronger (What Doesn't Kill You)

What went well? What didn't go well?

- Did you have an easy way to find vulnerable versions?
- Did you face friction from supporting teams?
- Did you have a communications plan in place?

What can be improved for next time?

- Plan to fix anything that didn't go well



Why do you write like you're running out of time?



**Document the
response efforts**



**Communicate results
with stakeholders and
customers**

**Create
templates**
for communication efforts

Write SOPs
on what to do in similar
situations



Friends in Low Places



It's Five O'clock Somewhere



**Take time to
breathe after an
incident**

**Mandatory fun
with your team**

99%

of people appreciate being
thanked for their hard work
after an incident

0%

of people will turn down
free food delivery



What comes next? (soon you'll see)



Questions?



Kennedy Toomey

AppSec Researcher & Advocate

@ Datadog



<https://kennedytoomey.github.io/bsidessf2026/>

