Customer Advisory: Shai-Hulud npm Supply Chain Attack – Our Security Review

Date: Sep 25, 2025

Executive Summary

We have completed a thorough review of our exposure to the recently disclosed **Shai-Hulud** npm supply chain attack. We compared all of our npm dependencies against the published lists of compromised packages and found no matches. We do not publish npm packages, we do not use GitHub, and we use an npm proxy to tightly control and audit our dependencies. Based on these measures, we have no evidence of compromise and our exposure to this attack is minimal.

Overview

The Shai-Hulud npm worm is a supply-chain attack that infects open-source JavaScript packages and can execute during installation. Once active, it can harvest credentials from developer or build environments and, in some cases, propagate to other packages under a compromised maintainer's control.

Although we do not publish npm packages or host our code on GitHub, we rely on open-source npm packages as part of our development environment. Because of this, we undertook a thorough review to ensure that our systems and data remain secure.

Actions We Have Taken

We collected published lists of compromised npm packages and versions from multiple trusted security sources, as well as a list of other known indicators of compromise. During scanning we have not found any matches or other suspicious indicators.

Because we do not publish npm packages, the self-replication mechanism of the Shai-Hulud worm cannot operate via our systems. We also do not use GitHub for our source repositories or CI/CD workflows, which prevents the worm from abusing GitHub-specific features to exfiltrate secrets or persist.

We use a controlled npm proxy to manage all npm packages used internally. This proxy caches approved versions of packages, enabling us to audit and control what enters our environment and preventing automatic downloads of unvetted versions.

Ongoing Monitoring

We continue to monitor updates to the list of compromised npm packages and review security advisories from npm, ReversingLabs, Wiz, JFrog, and other vendors. We also keep watch over our build environments for unusual package installs, outbound network traffic, or newly added scripts. Should any newly identified malicious packages overlap with our dependencies, we will immediately investigate and publish an update to this notice.

Customer Impact and Assurance

Currently, we have no evidence of compromise from the Shai-Hulud npm worm. Our use of an npm proxy and our policy of not publishing npm packages reduce our exposure to this class of attack. We will continue to monitor and update should anything change.