Published 12 Jul, 2018 under Postmortems

Postmortem for Malicious Packages Published on July 12th, 2018

Malicious versions of some ESLint packages were published (now unpublished) and we are sorry about this. We share details of the attack and our precautionary recommendations for package maintainers. Please check that you are not using the affected packages.

Contributors

Henry
@hzoo

Tags

security

Share

Summary

On July 12th, 2018, an attacker compromised the npm account of an ESLint maintainer and published malicious versions of the `eslint-scope` and `eslint-config-eslint` packages to the npm registry. On installation, the malicious packages downloaded and executed code from `pastebin.com` which sent the contents of the user's `.npmrc` file to the attacker. An `.npmrc` file typically contains access tokens for publishing to npm.

The malicious package versions are `eslint-scope@3.7.2` and `eslint-config-eslint@5.0.2`, both of which have been unpublished from npm. The `pastebin.com` paste linked in these packages has also been taken down.

npm has revoked all access tokens issued before 2018-07-12 12:30 UTC. As a result, all access tokens compromised by this attack should no longer be usable.

The maintainer whose account was compromised had reused their npm password on several other sites and did not have two-factor authentication enabled on their npm account.

> We, the ESLint team, are sorry for allowing this to happen. We hope that other package maintainers can learn from our mistakes and improve the security of the whole npm ecosystem.

Affected Packages

- `eslint-scope@3.7.` a scope analysis library, is a dependency of several popular packages, including some older versions of `eslint` and the latest versions of `babel-eslint` and `webpack`.
- `eslint-config-eslint@5.0` is a configuration used internally by the ESLint team, with very little usage elsewhere.

If you run your own npm registry, you should unpublish the malicious versions of each package. They have already been unpublished from the npmjs.com registry.

Attack Method

Further details on the attack can be found here.

Recommendations

With the hindsight of this incident, we have a few recommendations for npm package maintainers and users in the future:

- Package maintainers and users should avoid reusing the same password across multiple different sites. A password manager like 1Password or LastPass can help with this.
- Package maintainers should enable npm two-factor authentication. npm has a guide here.
  - If you use Lerna, you can follow this issue.
- Package maintainers should audit and limit the number of people who have access to publish on npm.
- Package maintainers should be careful with using any services that auto-merge dependency upgrades.
- Application developers should use a lockfile (`package-lock.json` or `yarn.lock`) to prevent the auto-install of new packages.

Timeline

- **Before the incident**: The attacker presumably found the maintainer's reused email and password in a third-party breach and used them to log in to the maintainer's npm account.
- **Early morning July 12th, 2018**: The attacker generated an authentication token in the maintainer's npm account.
- **2018-07-12 9:49 UTC**: The attacker used the generated authentication token to publish `eslint-config-eslint@5.0.2`, which contained a malicious `postinstall` script that attempts to exfiltrate the local machine's `.npmrc` authentication token.
- **2018-07-12 10:25 UTC**: The attacker unpublished `eslint-config-eslint@5.0.2`.
- **2018-07-12 10:40 UTC**: The attacker published `eslint-scope@3.7.2`, which contained the same malicious `postinstall` script.
- **2018-07-12 11:17 UTC**: A user posted eslint/eslint-scope#39, notifying the ESLint team of the issue.
- **2018-07-12 12:27 UTC**: The pastebin.com link containing malicious code was taken down.
- **2018-07-12 12:37 UTC**: The npm team unpublished `eslint-scope@3.7.2` after being contacted by an ESLint maintainer.
- **2018-07-12 17:41 UTC**: The ESLint team published `eslint-scope@3.7.3` with the code from `eslint-scope@3.7.1` so that caches could pick up the new version.
- **2018-07-12 18:42 UTC**: npm revoked all access tokens generated before 2018-07-12 12:30 UTC.

Links

- Original report: eslint/eslint-scope#39
- npm Status

Henry
Guest Author

Learning to maintain stuff

From the blog

The latest ESLint news, case studies, tutorials, and resources.

View all posts

Release Notes 1 min read

ESLint v9.13.0 released

We just pushed ESLint v9.13.0, which is a minor release upgrade of ESLint. This release adds some new features and fixes several bugs found in the previous release.

Francesco Trotta
18 Oct, 2024

Storytime 5 min read

no-unused-binary-expressions: From code review nit to ecosystem improvements

How implementing an ESLint rule led to changes in how people write JavaScript

Jordan Eldredge
08 Oct, 2024

Release Notes 2 min read

ESLint v9.12.0 released

We just pushed ESLint v9.12.0, which is a minor release upgrade of ESLint. This release adds some new features and fixes several bugs found in the previous release.

Francesco Trotta
04 Oct, 2024