Responsible Disclosure of Security Vulnerabilities

This document describes MyGet's policy towards Responsible Disclosure of Vulnerabilities.

MyGet does not run a bounty program. However, we want to keep MyGet safe for everyone. If you've discovered a security vulnerability in MyGet, we appreciate your help in disclosing it to us in a responsible manner.

MyGet Security contact info: info@myget.org

Last modified on 2017-11-09.

RULES FOR YOU

- Don't attempt to gain access to another user's account or data.
- Don't perform any attack that could harm the reliability/integrity of our services or data. DDoS/spam attacks are **NOT** allowed.
- Don't publicly disclose a bug before it has been fixed.
- Only test for vulnerabilities on sites you know to be operated by MyGet.
- Do not impact other users with your testing, this includes testing for vulnerabilities in package repositories you do not own. We may suspend your MyGet account and ban you IP address if you do so.
- Don't use scanners or automated tools to find vulnerabilities. They're noisy and we may suspend your MyGet account and ban your IP address.
- Never attempt non-technical attacks such as social engineering, phishing, or physical attacks against our employees, users, or infrastructure.
- When in doubt, contact us.

RULES FOR US

- We will respond as quickly as possible to your submission.
- We will keep you updated as we work to fix the bug you submitted.
- We will not take legal action against you if you play by the rules.

What does not qualify?

- Bugs that don't affect the latest version of modern browsers (Chrome, Firefox, Edge, Safari). Bugs related to browser extensions are also out of scope.
- Bugs requiring exceedingly unlikely user interaction.
- Bugs, such as timing attacks, that prove the existence of a private package repository or user.
- Insecure cookie settings for non-sensitive cookies.
- Disclosure of public information and information that does not present significant risk.
- Bugs that have already been submitted by another user, that we are already aware of, or that have been classified as ineligible.
- Bugs in content/services that are not owned/operated by MyGet. This includes our users' packages, and third-party services operating on subdomains of MyGet.org.
- Scripting or other automation and brute forcing of intended functionality.
- When in doubt, contact us.

Ineligible vulnerabilities

Impersonating a user through Personal Access Token

MyGet implements various package management protocols that may require the use of a Personal Access Token, oftentimes also referred to as 'API key', or just 'access token'. An example protocol that requires such token is the NuGet package push API.

MyGet has taken every possible precaution to secure these personal access tokens, and provides a variety of ways to reduce any potential attack surface that could be exposed in the event of a leaked access token.

In addition, and as explained in MyGet's Terms of Service, secure safeguarding and usage of such personal access token is a user responsibility.

Sharing a MyGet account and associated passwords, access tokens, or identities, is **strongly discouraged**, and makes it harder to revoke permissions, detect abuse, or control or determine damage as the result of leaked access tokens. As such, MyGet cannot be held responsible for any security vulnerability exposed by a leaked access token, whether accidentally or voluntarily.

However, MyGet takes security very seriously and will take corrective measure as soon as possible when informed about such situation. For example, we may immediately revoke the access token, block the user account or IP address, or even suspend access to the feeds this access token granted access to.

If you encounter a situation like this, do contact us with high priority!

FAQ

Am I eligible for some kind of bug bounty?

MyGet does not run a bug bounty program and does not provide any commitment in terms of rewards. This document merely describes MyGet's policy towards Responsible Disclosure of Vulnerabilities.

If you play by the rules, MyGet may, at its sole discretion, reward you for responsible disclosure of a security vulnerability. We are not a multi-million-dollar company, but we may reward the effort and ethical behavior shown of real security vulnerabilities found in our services.

In case a reward is granted, note that if you're under the age of 18 and live in the United States, you will need to submit a guardian consent form before any payment can be made. Individuals under 13 years of age are not eligible to participate due to U.S. federal law.

I reported a vulnerability but have not received a response!

Please allow up to 24 hours for an initial response. Also realize that spam filters and email in general can sometimes be problematic. If you ever feel we are not communicating in a timely fashion, definitely let us know.