WEBSITE VULNERABILITY DISCLOSURE

INFORMATION SERVICES GUIDE

About this guide

Introduction

1. If an external party discovers a vulnerability in any of Customs' external facing websites, we encourage them to report it.

2. Our aim is to ensure the security of our websites and any information they hold.

3. We also provide reassurance that Customs will not seek to prosecute people who find vulnerabilities and follow our guidelines in reporting them.

Overview

4. A website vulnerability is a weakness that allows an attacker to gain some level of control of a website. Once found, these vulnerabilities can be exploited to steal data, distribute malicious content, or inject defacement and spam content into the vulnerable site.

5. Customs has developed and deployed our websites to take current vulnerabilities into account. There are also processes in place with our suppliers to provide regular updates for vulnerabilities when they become known.

6. To complement these processes, we also encourage the public to notify Customs directly if they discover a vulnerability in one of our websites.

7. Some of Customs websites are complex and it will take time to investigate and resolve issues. When we're properly notified of legitimate issues, we aim to acknowledge your report, assign resources to investigate the issue and fix potential problems as quickly as possible.

Objectives

8. Customs will act in good faith with any party that reports a valid website vulnerability.

9. Customs would prefer an opportunity to investigate and resolve a vulnerability before details are made available to the public.

10. To maintain the security of our websites, we aim to investigate the cause of any reported vulnerabilities.

11. Customs will not seek legal recourse for any reported vulnerabilities unless the vulnerability is:

- used to change, deface or destroy the website
- used to corrupt or destroy data
- used to access or share any information that does not belong to the reporter
- reported to others so it may be exploited for malicious intent
- used to undertake ‘Denial of Service’ attacks.

Notify Customs

12. If you identify a website vulnerability, we need some information about the vulnerability. Please complete the website vulnerability form.

13. Customs will acknowledge receipt of this form as soon as possible and provide an update within seven (7) working days.

14. We will assess and validate the reported vulnerability.

15. If requested, you can be notified of the outcome.

16. Customs will aim to fix vulnerabilities as quickly as practicable.