EMEA INFORMATION SECURITY DEPARTMENT (EISD)

VULNERABILITY DISCLOSURE POLICY

April 2020

Public (R4)

Contents

Policy

Introduction

As Canon we take security of our IT systems seriously and values the security community. The disclosure of any security weaknesses helps us ensure the security and privacy of our users by acting as a trusted partner. This policy explains the requirement and mechanism related to Canon IT System Vulnerability Disclosure that allows researchers to evaluate Canon IT system to discover any vulnerability in a safe and ethical manner and report it to Canon Information Security team.

This Policy applies to everyone including internal Canon and external participants.

Canon IT Systems Vulnerability Disclosure Policy

The Canon Information Security team is committed to protect our employees & customers. As part of this commitment, we invite security researchers to help protect Canon and its users by proactively report security vulnerabilities and weaknesses. We work hard every day to maintain and improve our systems and processes so that our customers and partners can communicate and shop with us safely online. However, should you find a weakness in one of our IT systems, we always appreciate your help.

Reporting System Vulnerabilities

What you can report

You can report any number of weaknesses or vulnerabilities in Canon IT systems. If you spot a weakness, please contact us as soon as possible at product-security@canon-europe.com (see below par. for more details). Examples are:

- Cross-Site Scripting vulnerabilities (i.e. Stored, Reflected);
- SQL Injection vulnerabilities;
- Encryption weaknesses;
- Remote Code Execution;
- Use of broken algorithms:
- URL redirection of untrusted sites;

- Authentication Bypass, Unauthorized data access;
- XML External Entity;
- S3 Bucket Upload;
- Misconfigurations;
- Weak Passwords;
- Server-Side Request Forgery.

How to report a weakness

- Provide your IP address in the Weakness Report. This will be kept private for tracking your testing activities and to review the logs from our side.
- You can report weaknesses to us by email: product-security@canon-europe.com. Please state concisely in your email what weakness(es) you have found.
- Describe the found issue as explicit and detailed as possible and provide any evidence you might have, keeping in mind that the message will be reviewed by Canon Security specialists.
- We will not accept automated software scanners output.
- Particularly include the following in your e-mail:
  - The type of vulnerability;
  - The step by step instructions on how to reproduce the vulnerability;
  - Approach you undertook;
  - The entire URL;
  - Objects (as filters or entry fields) possibly involved;
  - Screen prints are highly appreciated.

What will not be accepted

- "Self" XSS;
- HTTP Host Header XSS without working proof-of-concept;
- Incomplete/Missing SPF/DKIM;
- Social Engineering attacks;
- Denial of Service attacks.
- Security Bugs in third part website that integrate with Canon.
- Mixed Content Scripts on www.canon.*
- Insecure Cookies on www.canon.*

What we do with your report

Canon Information security experts will investigate your report and will contact you within 5 working days.

Your privacy

We will only use your personal details to take action based on your report. We will not share your personal details with others without your express permission.

Rules

Potentially Illegal Actions

If you discover a weakness and investigate it, you might perform actions that are punishable by law. If you follow the rules and principles below for reporting weaknesses in our IT systems, we will not report your offence to the authorities and will not submit a claim.

It is important for you to know, however, that the public prosecutor's office – not CANON– may decide whether or not you will be prosecuted, even if we have not reported your offence to the authorities. Meaning we cannot guarantee that you will not be prosecuted if you commit a punishable offence when investigating a weakness.
The National Cyber Security Centre of the Ministry of Security and Justice has created guidelines for reporting weaknesses in IT systems. Our rules are based on these guidelines.

General Principles

Take responsibility and act with extreme care and caution. When investigating the matter, only use methods or techniques that are necessary in order to find or demonstrate the weaknesses.

- **Do not** use weaknesses you discover for purposes other than your own specific investigation.
- **Do not** use social engineering to gain access to a system.

- **Do not** install any back doors – not even to demonstrate the vulnerability of a system. Back doors will weaken the system's security.
- **Do not** alter or delete any information in the system. If you need to copy information for your investigation, never copy more than you need. If one record is sufficient, do not go any further.
- **Do not** alter the system in any way.
- Only infiltrate a system if absolutely necessary. If you do manage to infiltrate a system, do not share access with others.
- **Do not** use brute force techniques, such as repeatedly entering passwords, to gain access to systems.
- **Do not** use Denial of Service (DoS) type of attacks to gain access

Frequently-asked questions

Will I receive a reward for my investigation?

No, you are not entitled to any compensation.

Am I allowed to publicize the weaknesses I find and my investigation?

Never publicise weaknesses in Canon IT systems or your investigation without consulting us first via the email: product-security@canon-europe.com. We can work together to prevent criminals from abusing your information. Consult with our Information Security team and we can work together towards publication.

Can I report a weakness anonymously?

Yes, you can. You do not have to mention your name and contact details when you report a weakness. Please realise, however, that we will be unable to consult with you about follow-up measures, e.g. what we do about your report or further collaboration.

What shouldn't I use this email address for?

The email: product-security@canon-europe.com is not intended for the following:

- To submit complaints about Canon products or services
- To submit questions or complaints about the availability of Canon websites.
- To report fraud or suspicion of fraud
- To report phony emails or phishing emails
- To report viruses

Domains in scope

This is the list of domains which are included as part of the Canon Vulnerability Disclosure Policy.

- *.Canon-europe.com
- *.canon.nl
- *.canon.co.uk
- *.canon.com.tr
- *.canon.com.de
- *.canon.com.sa
- *.canon.com.ae
- *.canon.com.jp
- *.canon.com.ca
- *.canon.no
- *.canon.es
- *.canon.se
- *.canon.pl
- *.canon.be
- *.canon.pt
- *.canon.it
- *.canon.dk
- *.canon.ch
- *.canon.fi
- *.canon.at
- *.canon.fr
- *.canon.ie
- *.uaestore.canon.me.com