Vulnerability Reporting Policy

Introduction

Optum Services takes the protection of our customer and member data seriously. We are grateful for investigative work into security vulnerabilities that is carried out by well-intentioned, ethical security researchers. We are committed to collaborating with the information security community to investigate and resolve security issues within our web sites, online services, and mobile applications that are reported to us in accordance with this Vulnerability Reporting Policy. If you have information related to potential security vulnerabilities of Optum products or services, we want to hear from you.

Scope

This program is not intended for submitting complaints about Optum, or its subsidiaries' services or products, or for inquiries regarding the availability of company web sites or online services.

The following types of vulnerabilities are out of the scope for this program:

- Volumetric vulnerabilities (e.g., Denial of Service or Distributed DoS);
- Reports of non-exploitable vulnerabilities and violation of "best practices" (e.g. missing security headers);
- Transport Layer Security (TLS) configuration weaknesses (e.g., support for "weak" cipher suites);
- Fingerprinting/banner disclosure on common/public services;
- Self-cross-site scripting (XSS);
- Internal IP disclosure;
- Cross-site request forgery (CSRF);
- Un-exploitable HTTP Methods (e.g., OPTIONS or HEAD);
- Error-messages with non-sensitive data; and
- Lack of secure/HTTP-only flags on non-session cookies.

Optum may at any time update this policy, including the foregoing list of out-of-scope vulnerabilities.

Reporting a Vulnerability

If you have discovered an issue that you believe is an in-scope vulnerability, please email VulnerabilityReporting@optum.com. Please include the following, as applicable:

- A detailed description of the vulnerability
- The full URL
- A Proof of Concept (POC) or instructions (e.g. screen shots, video, etc.) on how to reproduce the vulnerability or steps taken

- Entry fields, filters, or other objects involved
- Risk or exportability assessment
- Instructions for how to reach you with follow up questions

Offering a solution is encouraged but not required. Lack of detailed vulnerability explanation may result in delays in our response and subsequent potential actions on the finding.

Bug Bounties

Optum does not currently offer a bug bounty program. However, we appreciate the efforts of security researchers who take time to investigate and report security vulnerabilities to us in accordance with this policy.

What to Expect

Upon receipt of the vulnerability report, Optum may send an automated response as acknowledgement. Optum may contact reporter(s) if additional information is needed to assist with the investigation. For the security of our customers, Optum will not disclose, discuss, or confirm security issues.

Public Notification

In order to protect our customers, Optum requests security researchers not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability and informed customers and stakeholders as needed. The time to address a valid, reported vulnerability will vary based on impact of the potential vulnerability and affected systems.

Guidance

This policy prohibits the performance of the following activities:

- Hack, penetrate, or otherwise attempt to gain unauthorized access to Optum software or systems;
- Active vulnerability scanning or testing;
- Disclose or use any proprietary or confidential Optum information or data, including customer data; or
- Adversely affect the operation of Optum software or systems.

Security researchers must not violate any law, or access, use, alter or compromise in any manner any Optum data.

If you have any questions regarding this policy or the guidance above, please contact our security team for guidance: VulnerabilityReporting@optum.com.

Policy Definitions

Vulnerability: A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events.

Denial of Service (DoS): An attack on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.

Distributed Denial of Service (DDoS): An attack on a service from multiple compromised computer systems that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate, thereby denying service to legitimate users or systems.

Transport Layer Security (TLS): A protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Self-Cross-Site Scripting (XCSS): A social engineering attack to gain control of a victim's web accounts via the victim unknowingly running malicious code on their own web browser.

Cross-Site Request Forgery (CSRF): A type of malicious exploit of a web site where unauthorized commands are transmitted from a user that the web site trusts. This is also known as a one-click attack or session riding.

Effective Date

The effective date of this policy is April 1, 2019.