UNIT4

In Business for You

Responsible Disclosure Procedure

9 May, 2024

Introduction

Unit4 is committed to identifying and resolving security issues in our systems and solutions in order to best protect our customers. We would like to collaborate with security researchers who may have found vulnerabilities in our systems before they can be exploited by attackers. This allows us to keep improving our processes, protect our data and customer data and maintain the availability of our services.

In Scope

If you have found a vulnerability in our security, please report this as soon as possible.

Examples are:

- Remote Code Execution
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- SQL Injection
- Encryption vulnerabilities
- Authentication bypasses and unauthorized data access.

Rules of Engagement

This procedure should be compatible with common good practice and does not give you permission to act in a way inconsistent with the law or cause Unit4 to be in breach of its legal obligations.

- Do not publish your report, but share it with us and allow time to resolve the issue.
- During investigation, do not apply any damage or changes in the system.
- Do not utilize social engineering in order to gain access to our systems.
- Your investigation should never disrupt our systems or services.
- Your investigation should never lead to the publicity of data.
- Do not place backdoors in systems.
- In case your finding requires a copy of the data from the system, do not copy more that your investigation requires.
- When reporting, do not include any personal information you may have obtained: e.g. blur names/e-mail addresses or redact the contents of server responses.
- Do not attempt to penetrate the system more than required and do not share gained access with others.
- Do not utilize any brute force techniques in order to gain access to the system.

Reporting

If you have discovered an in scope vulnerability, please send an encrypted email to security@unit4.com. Describe the issue as detailed as required and provide any evidence you might have including:

- Vulnerability identified
- The steps you took
- The entire URL
- Objects (as filters or entry fields) possibly involved
- Screen prints.

A team of security experts will verify your submission and respond as soon as possible. Please allow time to investigate (and resolve) the issue appropriately.

Rewards

Unit4 values the contributions of security researchers in identifying vulnerabilities in our products and processes. Eligible researchers who submit valid vulnerability reports may receive monetary rewards based on the severity and impact of the reported vulnerabilities. Our reward structure is designed to fairly compensate researchers for their efforts in enhancing the security of our services. We encourage security researchers to participate in our program and help us maintain the highest standards of security for our customers. Rewards may only be provided when a fix for the reported security bug is issued.

Confidentiality

Any information you receive or collect about Unit4 through the Responsible Disclosure program must be kept confidential and only used in connection with the program. You may not use, disclose or distribute any of this information, including, but not limited to, any information regarding your submission and information you obtain without Unit4's prior written consent.

Thank you for your help.