Process

BR-PROC-VRHP-2023

Vulnerability Reporting and Handling Process

TLP:WHITE

Can be distributed to the general public (incl. media).

17 February 2023

Traffic Light Protocol

RED	Do not distribute further, unless strictly necessary.
AMBER	Distribute only within the organisation and trusted partners.
GREEN	Can be distributed with related entities, but not the general public.
WHITE	Can be distributed to the general public (incl. media).
Not Rated	**Any document not rated should be considered TLP:RED**

Table 1 Document Control, Classification, and Distribution

Table of Contents

Tables

Figures

No table of figures entries found.

1. Introduction

This document outlines Blck Rhino Ltd.'s (BlckRhino) Vulnerability Reporting and Handling Process, designed to address security vulnerabilities discovered in systems associated with current and future technologies created and maintained by BlckRhino.

We subscribe to responsible disclosure and use GPG encryption for secure communication with researchers.

2. Scope

This process applies to vulnerabilities discovered in all systems enabling current and future technologies built by BlckRhino, including those involved in delivering products and/or services (free or paid) to existing or potential future customers, as well as the general public.

3. Communications

We are committed to resolving vulnerabilities promptly and effectively while maintaining open communication with the disclosing party. Although constant availability cannot be guaranteed, we will work diligently to overcome limitations, such as time-zone differences and language barriers, in order to facilitate the resolution process.

3.1 GPG Encryption for Secure Communication

We encourage security researchers to use GPG encryption when sending sensitive vulnerability information to our organisation.

Our GPG public key is available for download from our website here:

- https://www.blckrhino.com/security.asc

or can be found on multiple key servers using the email address:

- security@blckrhino.com

To import our GPG public key and encrypt your submission, you could follow these steps:

1. Download the GPG public key from the provided link or search for it on a key server using the associated email address.

2. Import the public key into your GPG keyring with the command:

```
# gpg --import security.asc
```

3. Compose your message, including details of the vulnerability and any supporting evidence.

4. Save the email content as a plain text file, e.g., 'vulnerability_report.txt'.

5. Encrypt the text file using our GPG public key with the command:

```
# gpg --encrypt --recipient security@blckrhino.com --armor --output
vulnerability_report.asc vulnerability_report.txt
```

6. Send the encrypted message (saved as 'vulnerability_report.asc') as an attachment to security@blckrhino.com and CC cvanniekerk@blckrhino.com.

4. Traceability and Accountability

We value the contributions of security researchers who report vulnerabilities and help us maintain a secure platform. To ensure visibility and accountability, we will assign a vulnerability identifier to each reported vulnerability, attributing it to the researcher who discovered it in all our internal tracking documentation as well as any public notifications that BlckRhino deems prudent.

5. Response Team

The initial response team will be made up of the Director of Product Development, and potentially other senior members of BlckRhino, who will assemble a Computer Emergency Response Team (CERT) with the relevant expertise to address the reported vulnerability. The response to reported vulnerabilities will be overseen by the highest levels within BlckRhino.

6. Responsible Disclosure

We believe in, and adhere to, the principles of responsible disclosure, working closely with security researchers to resolve identified vulnerabilities before any public disclosure. We will collaborate with the disclosing party to determine appropriate public disclosure timelines, giving proper credit to the researcher for their discovery. Our primary goal is to ensure the safety and security of our customers and systems.

7. Remediation and Closure

Upon receiving a vulnerability report, we will prioritise and remediate the issue based on its severity and potential impact. Once the vulnerability has been addressed, we will notify the

researcher and provide an update on the remediation status. In cases where a vulnerability requires additional time to resolve, we will maintain regular communication with the researcher to ensure transparency and collaboration throughout the process.

8. Continuous Improvement

We are committed to refining and improving our Vulnerability Reporting and Handling Process. We will periodically review and update our process based on feedback from researchers, internal teams, and industry best practices. Our goal is to foster a secure and robust environment for our customers and the broader community by promptly addressing vulnerabilities and continuously enhancing our security posture.

9. Contact Information

To report a vulnerability, please follow the GPG encryption process outlined in section 3.1 and send the encrypted message to security@blckrhino.com.

If you have any questions or concerns regarding this process or need assistance with GPG encryption, you can reach out to our team at the same email address.

We appreciate your support in helping us maintain a secure environment for our customers and the community.

10. Document Control and Classification

Classification	TLP:WHITE – Can be distributed to the general public (incl. media).			
Document Control	Initial Draft	0.1	2023-02-13	Colin van Niekerk
	Initial Release	1.0	2023-02-17	Colin van Niekerk

Table 2 Document Control and Classification