



VULNERABILITY DISCLOSURE POLICY

Nyansa is a data analytics solutions provider focused on discovering anomalies in our customers environments. As a provider of security services we take security issues very seriously, both discovered within our product and those we discover in our customer environments. It is our policy to work with all parties to ensure we are able to keep our customers, partners, and other third parties, including the public at large, safe and informed of any security issues. This document outlines our process for coordination and disclosure.

For issues discovered with a Nyansa product

If you believe you have found a vulnerability in any of Nyansa's products or have a security incident to report, please send an email to security@nyansa.com. After you make a report Nyansa will:

- Request that the report and all communication regarding the incident or vulnerability be kept confidential while Nyansa works to investigate and validate the report
- If the report or vulnerability cannot be patched quickly Nyansa will provide information regarding ways to mitigate risks associated with the reported incident or vulnerability
- Consider reports that contain more detail and demonstration of the reported vulnerability to be higher priority over other reports
- Work to keep you informed of the progress we are making and request you continue to maintain your confidentiality during this time
- When Nyansa publicly announces the vulnerability, we will give credit to the reporter or reporters who disclosed the vulnerability to Nyansa

Nyansa takes security seriously and appreciates the efforts of the security community to share information with us and giving us a chance to improve our products and secure our environments. We thank you for working with us with the above process.

For Security Issues found by Nyansa

As a security service provider Nyansa takes the discovery of security issues very seriously. It is our policy to work with our customers and other vendors when an issue or vulnerability is discovered. We make every attempt to resolve security issues directly with our customers and vendors and to allow third party vendors to work through their disclosure process.

At no time will Nyansa publicly disclose vulnerabilities found with our customer environments unless specifically authorized to do so through a release document.

Initial Contact

As we discover vulnerabilities in vendor products we will attempt to reach out to the vendor through their defined process if available, or we will use publicly available “contact us” information as found on their website. If the vendor provides a secure method of contact Nyansa will share our findings.

Nyansa will make multiple documented attempts to contact the vendor or third party. If no response is received from the vendor within two weeks, or if the vendor has ceased to communicate with Nyansa for a similar time period following an initial response, Nyansa may choose to release our findings publicly through a responsible disclosure process to notify and protect the greater public community.

Resolution

Nyansa will do our best to provide as much detail as we may be allowed to work with the appropriate vendor so they may develop a way to mitigate the risk and/or patch the vulnerability. At the end of the resolution or a period of 90 days, whichever is sooner, Nyansa may choose to publish our findings either through a public disclosure or via a private disclosure to our customers to better inform the community of the issue.

Third Party Disclosure

Nyansa may work with third parties to validate any discovery we make if we deem it is in the best interest of providing a more thorough response. Any disclosure to such third parties will be made responsibly and align to the above guidelines.

Nyansa will publish vulnerabilities on our website and in other communications as we deem it appropriate and responsible.