Comindware®

RESPONSIBLE DISCLOSURE

Comindware®

Effective Date: February 24, 2021

We take the security of our systems seriously, and we value the security community. Responsible disclosure of security vulnerabilities helps us ensure the security and privacy of our users.

Disclosure Policy

A security vulnerability is a weakness in the defenses of our services that may compromise the safety of our systems. Security researchers and others who become aware of potential vulnerabilities should make a report using the submission instructions below.

We encourage anyone who believes they have discovered a potential vulnerability, or who has become aware of unauthorized access to confidential Comindware data (including customer data), to inform us immediately to help protect our customers and to improve and strengthen the confidentiality, availability and integrity of our systems.

We promise to:

- Acknowledge receipt of reports in a timely manner
- Provide an estimated time frame for addressing a vulnerability report
- Notify you once the vulnerability has been fixed

Comindware does not offer a bug bounty program or compensation for disclosure.

Reporting Security Vulnerabilities

If you believe you've found a security vulnerability in our software please contact us. It will be very valuable to us, Reports should include the following information:

- Your name and contact information
- Your organization (if applicable)
- The Comindware services that may be affected
- A detailed description of the issue that you've discovered
- Supporting technical details, including descriptions or examples of exploit/attack code, packet captures, and steps to reproduce the issue
- Any known information about live exploits

Comindware®

Disclosure Guidelines

- We will promptly investigate all reports. If your report relates to a potential vulnerability, it should contain details sufficient for us to reproduce the vulnerability.
- We require a reasonable amount of time to remediate the situation before information about the issue is made known to the public.
- Do not engage in unauthorized data access, deletion, modification or corruption.
- Do not cause service disruptions while testing the vulnerability that you discovered.
- Prohibited research activities include denial of service, spamming, social engineering (including phishing), physical attempts against Comindware property or data centers, and other activities that may cause damage to Comindware's services, systems or to our or our customers' data, including activities that impact service availability, such as vulnerability scanning tools.
- Keep within the guidelines of our Terms Of Service.

Refrain from Public Disclosure

Taking into consideration the safety of our customers/users please do not publish any security vulnerabilities. We expect to fix all security issues within a reasonable amount of time days from the date of the reported security issue. Once an issue has been fixed we will explicitly acknowledge this and at which time you are free to publish your work.