Versasec Common Vulnerabilities and Exposures (CVE) Policy

	Name	Date	Comments
Created by	Anders Adolfsson	2024-11-19	
Reviewed by	Joakim Thorén	2024-11-19	
Updated by			
Status			
Classification	External		

Introduction

At Versasec, we prioritise the security and integrity of our products. We recognize that vulnerabilities can emerge in any software or hardware, and we are committed to proactively identifying, assessing, and addressing these issues to protect our customers. This CVE Policy outlines our approach to managing and disclosing vulnerabilities in a transparent and responsible manner.

Scope

This policy applies to all Versasec products. We are dedicated to maintaining the highest security standards across our entire product portfolio.

Vulnerability Identification and Assessment

- **Internal and External Sources:** We leverage a multi-pronged approach to identify potential vulnerabilities. This includes rigorous internal testing, as well as active engagement with the security research community, partners, and customers. We encourage responsible disclosure of any potential vulnerabilities. See: https://versasec.com/about-versasec/disclosure-policy/
- **Thorough Assessment:** Each reported vulnerability undergoes a meticulous assessment by our security experts. We use industry-standard methodologies, such as the Common Vulnerability Scoring System (CVSS), to evaluate the severity and potential impact of the issue.

Severity Classification

- **Clear and Actionable:** To provide our customers with a clear understanding of the potential risks, we classify vulnerabilities based on their severity:
    - **Critical:** Vulnerabilities that pose a significant risk of exploitation, potentially leading to severe data breaches, system compromise, or service disruption.
    - **High:** Vulnerabilities that could be exploited to gain unauthorised access, modify data, or cause significant operational disruptions.
    - **Medium:** Vulnerabilities that may allow limited unauthorised access or data manipulation, but with less severe consequences.
    - **Low:** Vulnerabilities that have minimal impact on the confidentiality, integrity, or availability of our products or services.

Vulnerability Remediation and Patching

- **Rapid Response:** We are committed to addressing vulnerabilities promptly and effectively. Our response timeframes are aligned with industry best practices:
    - **Critical and High-Severity Vulnerabilities:** We strive to develop and release patches or mitigation strategies within 30 days of assessment, or sooner if possible.
    - **Medium and Low-Severity Vulnerabilities:** We aim to address these vulnerabilities in our regular update cycles, or sooner if warranted by the specific circumstances.
- **Thorough Testing:** All patches and updates undergo rigorous testing to ensure their effectiveness, compatibility, and stability before being released to our customers.

CVE Publication and Customer Notification

- **Transparency and Clarity:** We believe in open communication with our customers. When a vulnerability is identified and remediated, we assign a CVE ID (when applicable) and publish a detailed security advisory on our support portal. This advisory includes:
    - A clear description of the vulnerability.
    - The assigned CVE ID.
    - Affected products and versions.
    - The potential impact of the vulnerability.
    - Recommended mitigation strategies or steps to apply the patch.
- **Proactive Communication:** We notify our customers about security updates through multiple channels, including:
    - Email notifications to registered users.
    - Announcements on our support portal.
    - Release notes accompanying product updates.

Reporting a Vulnerability

- **Responsible Disclosure:** We encourage security researchers, partners, and customers to report potential vulnerabilities to us in a responsible manner. Please submit your findings to our dedicated security email address: info@versasec.com.
- **Prompt Acknowledgement and Investigation:** Our security team will acknowledge your report promptly, investigate the issue thoroughly, and keep you informed of the progress.

Customer Responsibility

- **Stay Updated:** We urge our customers to apply security updates as soon as they are available. Regularly updating to the latest versions of our products ensures that you benefit from the most recent security enhancements.

- **Follow Best Practices:** We recommend following our security advisories and guidance to further enhance the security of your Versasec deployments.

Policy Updates

- **Continuous Improvement:** This policy may be updated periodically to reflect evolving industry standards, regulatory requirements, or changes in our product offerings. We will always maintain the latest version on our website.

Contact Us

- **We're Here to Help:** If you have any questions or concerns regarding this CVE Policy or any security-related matters, please don't hesitate to contact our Customer Support team or reach out to us via email at support@versasec.com

By adhering to this comprehensive CVE Policy, Versasec demonstrates its unwavering commitment to product security, customer trust, and responsible disclosure practices.