Comba Security Vulnerability Reporting Template v1.0

Thank you for reporting potential security vulnerabilities in Comba products.

This template is designed to help security researchers, customers, and partners provide the necessary information for vulnerability validation, assessment, and remediation. Providing complete and accurate information will help us investigate and address reported security issues more efficiently. *(Note: * Required)*

1. Reporter Information (You may submit reports anonymously. However, if you choose not to provide contact information, we may be unable to provide updates regarding vulnerability investigation and remediation progress.)			
Name		**Organization**	
Email Address		**Preferred Contact Method**	
2. Vulnerability Information*			
Affective Product / Component Information			
Product / Component Name			
Product Type	☐ Hardware ☐ Firmware ☐ Software ☐ Remote Network Management System		
Model Number			
Firmware / Software Version			
Vulnerability Details			
Vulnerability Name			
Vulnerability Category	☐ Remote Code Execution (RCE) ☐ SQL Injection ☐ Cross-Site Scripting (XSS) ☐ Privilege Escalation ☐ Command Injection ☐ Broken Access Control ☐ Weak Password ☐ Other: _____		

Risk Severity	
☐ Critical ☐ High ☐ Medium ☐ Low	
Vulnerability Description Please provide: - Vulnerability overview - Potential impact - Affected functions/components	
Technical Details and Reproduction Steps Please provide: - Detailed technical information - Reproduction steps - Testing environment - Preconditions required for exploitation	
Proof of Concept (POC/EXP) Please provide: - POC code - Exploit information - Demonstration video - Related links	
Attachment (Optional) Examples: - Screenshots - Logs - Network capture files - Supporting documents	

3. Vulnerability Impact Assessment

Please describe the potential impact of this vulnerability, including:

- Possible attack scenarios
- Affected users/Products
- Security impact (confidentiality, integrity, availability)

4. Recommended Fixes or Mitigation Suggestions

If available, please provide recommended fixes, solutions, or temporary mitigation measures.

5. Disclosure Preference

Have you planned to publicly disclose this vulnerability after remediation?

☐ Yes

☐ No

Please do not publicly disclose vulnerability details before remediation is completed and coordinated with Comba.

6. Public Acknowledgement Preference

Would you like to be publicly acknowledged in Comba Security Advisories?

☐ Yes. Preferred name/nickname:

☐ No

7. Additional Information

Please provide any additional information that may help us understand, verify, or resolve the reported vulnerability.

Thank you for helping Comba improve product security. We appreciate responsible vulnerability disclosure from the security community and will make reasonable efforts to investigate and address reported security issues according to our Coordinated Vulnerability Disclosure Policy.