Suspected Vulnerability Reporting

Template v1.0

Thank you for reporting the suspected security vulnerability in MAXHUB products and solutions. This template is designed to facilitate the verification and location of suspected security vulnerabilities.

1. Personal or organizational information	
Name (optional)	Contact information (required)
	This will be used to facilitate further communication with you in scenarios such as problem localization.
2. Vulnerability Information	
Affected MAXHUB related products or components This information is used to help us quickly locate the affected products . Please provide the specific MAXHUB product or component name .	
Brief description of the vulnerability Please describe the vulnerability as briefly as possible , including the type of vulnerability and the potential impact of an attacker successfully exploiting it.	
Vulnerability Technical Details Please provide the technical details of this vulnerability , including the following: 1. A detailed description of the vulnerability's technical aspects; 2. Detailed steps to reproduce the vulnerability (this will be crucial for us to reproduce your findings) ; 3. If you can provide a Proof of Concept (PoC), please send it to us as an additional attachment to this report.	
vulnerability attack scenarios A vulnerability attack scenario differs from a vulnerability reproduction step . It describes how an attacker can successfully exploit the vulnerability . It includes the preconditions for the attacker to launch an attack, the restrictions on vulnerability triggering , and whether interaction with the victim is required . Describing vulnerability attack scenarios will help us quickly assess your security report,	

especially for complex security issues.
Recommendations for repair and mitigation measures This content can help us understand how to fix vulnerabilities , including detailed remediation methods, solutions , industry best practices , and temporary mitigation measures such as IPS /WAF rule formulation .
3. Vulnerability Disclosure
Do you have any plans to publicly discuss this vulnerability after it has been patched , including giving presentations at conferences, publishing technical articles, etc.? Please select the corresponding option . Please note that we require that you not disclose the security vulnerability you reported to any third party (including any third party other than yourself) until it has been patched. If you intend to publicly discuss the vulnerability after we have patched it, including through conference presentations, publishing technical articles, etc., please contact security@maxhub.com in advance .
☐ Yes ☐ No
4. Is it permissible to express gratitude externally? **In principle, the security bulletin publicly disclosed regarding this vulnerability will include a thank you note. Do you agree?**

☐ Yes	Please provide the name or nickname of the person you wish to thank.
☐ No	

5. Other Information Any information you deem necessary that is not covered in the information above

The policy descriptions in this document do not constitute guarantees or commitments, and MAXHUB may adjust the above policies at its discretion. Users assume all risks when using the information in this document or the materials linked in this document. MAXHUB reserves the right to change or update this document at any time, and we will

update this policy statement as necessary to increase transparency or respond more proactively.