3JCNS Vulnerability Disclosure Policy
(취약점 공개 및 신고 정책)

Date: 2025.12.05

1. Introduction (개요)

3JCNS takes the security of our systems and our customers' data seriously. We value the assistance of security researchers and the community in identifying potential vulnerabilities in our Plant IT Solutions. This policy outlines how to report vulnerabilities to us.

2. Scope (범위)

- In Scope:
  3JCNS Web Applications, API endpoints provided to clients, Official website.
- Out of Scope:
  DDoS attacks, Social Engineering (Phishing), Physical security attacks.

3. Reporting a Vulnerability (신고 방법)

If you believe you have found a security vulnerability in a 3JCNS product or service, please report it to us immediately via email.

- Email: d.shin@3jcns.com
- Content: Please include a description of the vulnerability, steps to reproduce, and proof-of-concept (PoC) code/screenshots.

4. Our Commitment (당사의 약속)

- We will acknowledge receipt of your report within 5 business days.
- We will provide an estimated timeline for the fix.
- We will notify you once the vulnerability is patched.

5. Safe Harbor (면책 조항)

3JCNS will not pursue legal action against researchers who:

- Report vulnerabilities in good faith to help us fix them.
- Do not exploit the vulnerability to view, modify, or delete data beyond what is

necessary to prove the issue.

- Do not disclose the issue to the public until 3JCNS has had a reasonable time to fix it.

쓰리제이씨앤에스 주식회사

3JCNS Co., Ltd.

3JCNS Co., Ltd.
(Reg.No. 220-88-18359)
2F, 234, Teheran-ro, Gangnam-gu,
Seoul, KOREA
Tel: +82 (0)2 2183-2861
Fax: +82 (0)2 2183 2863