EMP / Concentric Product Cybersecurity Vulnerability & Incident Reporting

Purpose

Concentric and EMP are committed to the timely identification, assessment, and resolution of product cybersecurity vulnerabilities and security incidents.

This reporting process is intended for customers, suppliers, business partners, researchers, distributors, employees, and other parties who become aware of a potential cybersecurity issue affecting an EMP or Concentric product.

Reports submitted through this process will be reviewed and escalated to the appropriate product cybersecurity contacts for evaluation and response.

What Should Be Reported?

Please report any known or suspected cybersecurity vulnerability or security incident involving an EMP or Concentric product, including but not limited to:

- Unauthorized access to a product or device
- Suspected malicious activity affecting a product
- Cybersecurity weaknesses or vulnerabilities
- Security configuration concerns
- Software or firmware vulnerabilities
- Evidence of attempted exploitation
- Suspected compromise of product functionality
- Security concerns identified during testing or research
- Any cybersecurity issue that may affect product security, reliability, availability, or integrity

If you are uncertain whether an issue should be reported, please submit a report. The Product Security Team will review the information and determine the appropriate response.

Submit a Report

Preferred Reporting Method

Please submit cybersecurity vulnerabilities and incidents using the reporting form below:

Product Cybersecurity Reporting Form

Use → THIS FORM ←

Using the reporting form helps ensure:

- Immediate notification of the appropriate personnel
- Continuous coverage during absences or out-of-office periods
- Proper escalation and tracking
- Accurate documentation for investigation and response
- Faster coordination with product cybersecurity teams

Information to Include

Please provide as much information as possible.

Reporter Information

- Name
- Organization or company
- Email address
- Telephone number (optional)

Product Information

- Product name
- Full Part number
- Serial number

Issue Details

- Description of the vulnerability or incident
- Date discovered
- How the issue was identified
- Whether the issue is currently being exploited (if known)

- Known or suspected impact
- Any actions already taken

Supporting Information

If available, please provide:

- Screenshots
- Log files
- Diagnostic information
- Technical reports
- Proof-of-concept information
- Photograph of product label
- Other supporting documentation

What Happens After Submission?

After a report is received:

1. The information will be reviewed by the designated Product Cybersecurity contacts.
2. The issue will be assessed to determine potential impact and severity.
3. Additional information may be requested if needed.
4. Appropriate investigation, mitigation, and response activities will be initiated.
5. Regulatory reporting requirements, where applicable, will be addressed by the responsible organization.

Submission of a report does not necessarily indicate that a vulnerability or cybersecurity incident has been confirmed.

Confidentiality

Information submitted through this reporting process will be handled in accordance with applicable company policies and legal requirements.

Please do not include confidential information that is unrelated to the reported cybersecurity issue.

Alternative Contact Method

If you are unable to access the reporting form, cybersecurity concerns may be reported using the contact information below.

Product Cybersecurity Contact

Email: **productsecurity@emp-corp.com**

Deputy Contacts

Email: Jacob.Smith@emp-corp.com; Robert.Cox@emp-corp

Emergency Situations

If you believe a cybersecurity issue is being actively exploited or presents an immediate and significant risk to customers, products, or operations, please submit the reporting form immediately and indicate that active exploitation is suspected.

EMP / Concentric Product Cybersecurity Reporting
Version 1.0
Effective Date: September 2026