Mallinckrodt Cybersecurity: Vulnerability Reporting

Mallinckrodt is committed to delivering safe and secure products and services. When vulnerabilities are discovered, we work diligently to resolve them. This document describes Mallinckrodt's assurance for receiving reports related to potential security vulnerabilities in its products, services and websites and the company's standard practice with regards to informing customers of verified vulnerabilities. Mallinckrodt gives vulnerability reporting the necessary due diligence needed and we will report any disclosures of vulnerabilities that are found to be true and accurate.

When to contact Mallinckrodt regarding a Vulnerability
Contact Mallinckrodt by sending an email to mpvr@mnk.com if you have identified a potential security vulnerability with one of our products, services or websites; include **"VULNERABILITY DISCLOSURE"**. After your incident report is received, the appropriate personnel will contact you to follow-up.

To ensure confidentiality, we encourage you to encrypt any sensitive information you send to us via email.

Mallinckrodt Responsibilities
The mpvr@mnk.com email address is intended ONLY for the purpose of reporting security vulnerabilities specific to our products or services. For technical support information on our products or services, please visit https://mnk.com/.

Mallinckrodt strives to acknowledge receipt of all submitted reports within three business days.

To the best of our ability, we will confirm the existence of the security vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including issues or challenges that may delay resolution.

We will maintain an open dialogue to discuss issues.

What We Would Like From You

To help us triage and prioritize submissions, a report detailing your security research should include, at a minimum, the following:
- Describe the security vulnerability, where it was discovered, and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the security vulnerability (for example proof of concept scripts or screenshots).
- A clear and detailed description of the security vulnerability.
- Clear and detailed information about how the security vulnerability has been discovered. The objective is to be able to reproduce it.
- Proof of the existence of the security vulnerability (screenshot, link, etc.)
- A timeline or other information about the moment (date and time) the security vulnerability was discovered.
- All information necessary for locating and resolving the security vulnerability in the fastest and most efficient way possible.
- Be in English, if possible.

Security Advisories

If warranted Mallinckrodt will communicate newly identified vulnerabilities to reporting organizations. This may include CISA (Cybersecurity and Infrastructure Security Agency) and other vulnerability information sharing organizations. In cases where there are regulatory or legal requirements to report security research findings, Mallinckrodt will report such findings to the appropriate agencies.

In cases where a third party notifies Mallinckrodt of a potential vulnerability found in our products we will investigate the finding and may publish a coordinated disclosure along with the third party. In some instances, Mallinckrodt may receive information about a security vulnerability from a supplier under a confidentiality or non-disclosure agreement or under embargo. In these cases, Mallinckrodt will work with the supplier to request that a security fix is released although we may not be able to provide details

about the security vulnerability. Mallinckrodt does not publish security advisories for open source vulnerabilities.

Severity

In scoring or rating vulnerabilities, Mallinckrodt follows standard industry best practices to designate the vulnerability's potential impact as High, Medium or Low. This approach follows the Common Vulnerability Scoring System (CVSS), which provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors, and researchers to all benefit by adopting a common language of scoring IT vulnerabilities.

References

If additional information on the vulnerability is available, the advisory will provide links as a reference. This includes links to the CVE or blog or article citations.

Acknowledgement

Typically, we look to acknowledge the researcher or finder of the vulnerability and, with their permission, will credit them.