NILFISK

Nilfisk Information Security Vulnerability Disclosure Policy

Contents

1 Introduction

1.1 About Nilfisk

Nilfisk Group (hereby after the “Organization”) is a leading provider of professional cleaning products and services.

The company was founded on a vision of producing and selling products of the highest quality worldwide and for more than a hundred years, Nilfisk has adapted to the changing needs of markets and customers with innovative products and solutions. With a global sales force and proven sales channels, we have established strong and valuable customer relations and partnerships across the world, and we strive to be at the forefront of technological advancement to drive future customer needs.

Today, Nilfisk offers an extensive range of premium cleaning products and a trusted aftermarket offering to the professional market. Our main product lines are floorcare equipment, vacuum cleaners and high-pressure washers and a wide range of domestic vacuum cleaners and high-pressure washers for consumers worldwide.

1.2 About this policy

This vulnerability disclosure policy applies to any vulnerabilities you (a party not employed by or working on behalf of Nilfisk) are considering reporting to us (the "Organization"). We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it.

We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

2 Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following email: infosec@nilfisk.com

In your report, please include details of:

- The website, IP, or page where the vulnerability can be observed.
- A brief description of the type of vulnerability, for example; “XSS vulnerability”.
- Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.
- Recommendations how to remediate the vulnerability. This helps to speed-up any remediation process and give a hint to our developers to do it quicker.

3 What to expect

After you have submitted your report, we will respond to your report within 10 working days and aim to triage your report within 10 working days. We will also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Nilfisk requests that you not publicize or share with others any report you make about a Nilfisk vulnerability. Doing so might expose Nilfisk to hacking or other cyber-attacks.

You may not publicize or share e-mail or text communication from Nilfisk systems, or any Nilfisk personal data or any other Nilfisk information that Nilfisk has not already made public, including financial data or information about its customers, vendors or investors.

4 Guidance

You must NOT:

- Violate any applicable law or regulations.
- Access data unnecessary to identifying the vulnerability, or excessive or significant amounts of data.
- Access any personal data in any Nilfisk system.
- Modify data in the Organization's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g., overwhelming a service with a high volume of requests.
- Disrupt the Organization's services or systems.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with “best practice”, for example missing security headers.
- Submit reports detailing TLS configuration weaknesses, for example “weak” cipher suite support or the presence of TLS1.0 support.
- Communicate any vulnerabilities or associated details other than by means described in the published security.txt.
- Social engineer, ‘phish’ or physically attack the Organization's staff or infrastructure.
- Demand financial compensation in order to disclose any vulnerabilities.
- Test domains and report vulnerabilities which are not listed in section “5 Scope”.
- Disclose any reported or/and unreported findings.

You must:

- Always comply with data protection laws and regulations and must not violate the privacy of the Organization's users, employees, vendors, contractors, customers (including dealers), services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 week of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).
- Only report bugs on the domains listed in section “5 Scope”.

5 Scope

The following web domains are in scope for this policy:

Site / domain name
nilfisk.com
densin.com
splashequip.co.nz
www.industroclean.co.za
www.wap-waschbaer.org
www.nilfisk-advance.com.tw
www.nilfisklibertya50.nilfisk.de

nilfiskdemos.ca
nilfisk-zentralstaubsauger.at
magnum-pressurepro.com
nilfiskfood.com
www.nilfisk-frithiof.dk
nilfisk-advance.com.br
viperbrasil.com.br
www.mujnilfisk.cz
www.nilfisktrackclean.com
www.kerrick.com.au
https://www.jessica-viper.com.tw/
www.nilfiskkozponti.hu
smil-alto.fr
www.nilfisk-conso.fr
gesco.be
www.nilfisk.us
www.nilfiskcfm.com
www.gerni.com.au
www.nilfiskcleaning.com
www.nilfisk.com.ar
nilfisk.tw
www.advance-ca.com
www.clarke-ca.com
nilfisku.com
magnumpressurewashers.com
webshop.nilfisk.hu
consumer.nilfisk.com.au
www.vipercleaning.com.ar

6 Legalities

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause the Organization or affiliated companies or its business partners to be in breach of any legal obligations.