



gewählten Cookie-Präferenzen. Wir bitten Sie, dass Sie die volle Funktionalität unserer personalisierte Nutzererlebnis dieser Website nicht zur Verfügung stehen.

## Article

Weitere Informationen finden Sie im [Cookie-Hinweis](#).

## Nozomi Stored XSS

A stored Cross-Site Scripting (XSS) vulnerability in the Nozomi Network's Guardian OS web application allows an attacker to inject JavaScript into the website. This may allow a malicious entity to gain (administrative) access to the application or perform actions on behalf of the victim user.

## Background

We discovered a security issue in the Nozomi Network Guardian OS web interface. It is possible to inject JavaScript code within the function to create custom fields for the e.g. environment overview of the product due to a lack of sufficient input filtering. An attacker can inject malicious code that will later be executed by legitimate users who open the website. An attacker may perform unauthorized actions on behalf of legitimate users or spread malware via the application.

## Steps to Reproduce

The application performs filtering of XSS and other injection vectors. However, this filtering somehow was not applied to this input field as well. We were able to use the put JavaScript without whitespaces and limited characters to circumvent the protection. This results in successful stored XSS.

The characters , ' and " within the payload will most likely lead to not trigger the XSS.

The following pictures show how we were able to exploit the vulnerability.

## Root Cause

This issue exists due to insufficient input filtering in the input field of the custom field section. In order to mitigate the issue, we recommend applying input filtering to all input fields and URL parameters in the entire application to ensure that only valid input is processed (this means input filtering for the fields as well as for the field values).

## Fix

We were able to verify this vulnerability in software versions below 19.0.3. However, all versions below 19.0.4 are likely affected. The vendor was informed of the finding and already implemented a fix for this issue. Therefore, updating to version 19.0.4 will mitigate the issue successfully.

## Credit

Credit for finding and reporting the issue:

**Jonas Becker**

## Ihre Ansprechpartner



**Peter J. Wirsperger**  
Partner | Public Sector  
pwirsperger@deloitte.de  
+49 40 320804675



Peter Wirsperger leitet den Bereich Civil Government und ist als Mitglied des Führungsteams von Risk Advisory verantwortlich für die Themen strategische Entwicklung und Innovation. Er ist seit 2003 b... Mehr



**Murat Yildiz**  
Partner | Cyber  
myildiz@deloitte.de  
+49 6211590125



Murat Yildiz führt das lokale Cyber Intelligence Center Team in Deutschland, wobei er sich mit Themen wie SOC / SIEM, Threat Intelligence, Penetration Testing, Source Code Review usw. beschäftigt. Her... Mehr

## Auch interessant

[Home](#)

[Über Deloitte Deutschland](#)

[Deloitte-Stiftung](#)

[Alumni](#)

[Events](#)

[Pressemitteilungen](#)

[Blogs](#)

[Podcasts](#)







[Angebotsanfrage](#)

# Deloitte.

## Ihre Datenschutz-Einstellungen

Deloitte setzt Cookies ein, um die einwandfreie Funktion unserer Webseite zu gewährleisten, statistische Analysen zur Optimierung unserer Webseite durchzuführen und zusammen mit Drittanbietern Inhalte und Werbung zu personalisieren.

Wenn Sie auf **"Alle Cookies akzeptieren"** klicken, stimmen Sie der Platzierung dieser Cookies auf Ihrem Gerät zu. Sie können diese Cookies jederzeit ablehnen oder verwalten, indem Sie auf **"Cookie-Einstellungen"** klicken. Je nach den von Ihnen gewählten Cookie-Präferenzen kann es sein, dass die volle Funktionalität oder das personalisierte Nutzererlebnis dieser Website nicht zur Verfügung stehen.

-  <https://www.facebook.com/Deloitte.Deutschland>
-  <https://twitter.com/DeloitteDE>
-  <https://www.linkedin.com/company/deloitte/>
-  <https://www.xing.com/company/deloitte>
-  <https://www.instagram.com/deloittedeutschlandkarriere/>
-  <http://www.youtube.com/user/DeloitteDeutschland>

Weitere Informationen finden Sie im [Cookie-Hinweis](#).

## Services

[Audit & Assurance](#)

[Risk Advisory](#)

[Tax](#)

[Legal](#)

[Financial Advisory](#)

[Consulting](#)

[Deloitte Private \(Mittelstand\)](#)

[Spotlight](#)

## Industries

[Consumer](#)

[Energy, Resources & Industrials](#)

[Financial Services](#)

[Government & Public Services](#)

[Life Sciences & Health Care](#)

[Technology, Media & Telecommunications](#)

## Careers

[Jobsuche](#)

[Berufserfahrene](#)

[Studierende](#)

[Karriere bei Deloitte](#)

[Schüler:innen](#)

[Absolvent:innen](#)