



personalisierte Nutzererlebnis dieser Website nicht zur Verfügung stehen.

Article

Weitere Informationen finden Sie im Cookie-Hinweis.

Nozomi CSV Injection

Alle Cookies akzeptieren

A CSV injection in the Nozomi Networks Guardian OS from Nozomi Networks allows malicious users to gain renote control of other computers. By choosing fight and core as label for different entries, an attacker can create flag entries within the environment overview with malicious code. Other users might download this data as a CSV file and corrupt their PC by opening it in a tool such as Microsoft Excel. The attacker could gain remote access to the user's PC.

Background

We discovered a security issue within the Nozomi Networks Guardian OS Web Interface in versions < 19.0.4 from Nozomi Networks, a product for monitoring industrial environments (OT). An attacker can input malicious formula data due to a lack of sufficient input filtering. This allows attacking clients who export the data as a CSY file and open in it so tools like Microsoft Excel or LibreOffice Calc. The attacker can infect users with malware and gain control over their host computers, if the malicious code is executed successfully.

Steps to Reproduce

Upon creating a new user account, a malicious user is able to put formula code into the field for labels. Users that are authorized could export and download all the entries from e.g. environment tab at the system as a CSV file. Even though, the user will hide the label section, it will still be exported. If the infected CSV file is opened with Microsoft Excel, the malicious formula code will be executed. In this example, the label =cmd | 7 C notepad?N1' was involved in an action. In excel the formula is interpreted and executed by Excel.

Root Cause

This issue exists due to insufficient input filtering. In order to mitigate the issue, we recommend sanitizing cells that begin with any special character that might trigger the creation of a formula such as "=", "+", "@" or "-", by prepending a single quote or apostrophe () character to it, in order to avoid the content of the cell being interpreted as a formula.

Fix

The issue was reported to Nozomi Networks and fixed in the version 19.0.4 of their OS Nozomi Networks Guardian

Therefore, we recommend updating the software to the latest stable release

Credit

Credit for finding and reporting the issue:

Ihre Ansprechpartner



Peter J. Wirnsperger Partner | Public Secto pwirnsperger@deloitte.de +49 40 320804675



Peter Wirnsperger 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



Christian Duewel Director | Cyber Defense & Managed Security Services cduewel@deloitte.de +49 40 320804138



Christian ist Director im Bereich Cyber Defense und Managed Security Service mit mehr als 20 Jahren umfassender praktischer Erfahrung im Bereich Cybersicherheit. Sein Fokus liegt auf der Entwicklung u... Mehr

Auch interessant

Jobsuche Kontakt Angebotsanfrage Newsletter

Über Deloitte Deutschland

Deloitte-Stiftung Deloitte.

Alumni Ihre Datenschutz-Einstellungen

Events Deloitte setzt Cookies ein, um die einwandfreie Funktion unserer Webseite zu Pressemitteilungen

⊕ DE-DE
✓

gewährleisten, statistische Analysen zur Optimierung unserer Webseite durchzuführen

und zusammen mit Drittanbietern Inhalte und Werbung zu personalisieren. Blogs

Podcasts Wenn Sie auf "Alle Cookies akzeptieren" klicken, stimmen Sie der Platzierung dieser Cookies auf Ihrem Gerät zu. Sie können diese Cookies jederzeit ablehnen oder Angebotsanfrage

verwalten, indem Sie auf **"Cookie-Einstellungen"** klicken. Je nach den von Ihnen gewählten Cookie-Präferenzen kann es sein, dass die volle Funktionalität oder das

https://www.facebook.com/Deloitte.DeutsPMSSQnalisierte Nutzererlebnis dieser Website nicht zur Verfügung stehen.

Weitere Informationen finden Sie im Cookie-Hinweis. 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

Services

Audit & Assurance

Risk Advisory

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

Iobsuche

Berufserfahrene

Studierende

Karriere bei Deloitte

Schüler:innen

Absolvent:innen

Über Deloitte \parallel Rechtliche Hinweise \parallel Cookies \parallel Impressum \parallel Datenschutzhinweise

© 2022. See Terms of Use for more information.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/de/about to learn more about our global network of member firms.