



Thema:
**Information zur aktuellen Log4Shell-/Log4j-Schwachstelle
- Datafox Produkte NICHT betroffen**

Sehr geehrter Datafox Kunde,

Sie verwenden Hardware von Datafox oder haben in der Vergangenheit Geräte von uns erworben. Aus diesem Grund möchten wir Sie darüber informieren, dass Datafox Produkte (Datafox **Hardware**, die Datafox **Kommunikationsbibliothek**, Datafox **Talk** und das **DatafoxStudioIV**) von der aktuellen Log4Shell (CVE-2021-44228) Schwachstelle **NICHT** betroffen sind.



Info: Log4Shell (CVE-2021-44228)

Worum handelt es sich bei der Log4Shell-Schwachstelle?

Bei der Log4Shell-Schwachstelle handelt es sich zusammengefasst um eine Computer- bzw. Hardware-Schwachstelle, welche Hacker gezielt angreifen können, um unbemerkt die Kontrolle oder Fernsteuerung über fremde Geräte zu erlangen. Das Bundesamt für

Sicherheit (BSI) stuft die Log4Shell-Schwachstelle als besonders kritisch ein und hat eine ohnehin bestehende Cyber-Sicherheitswarnung auf die Warnstufe ROT erhöht.

Wie bereits oben im Text erwähnt, sind Datafox Produkte **NICHT** von dieser Schwachstelle betroffen. Wir hoffen, dass Sie und Ihr Unternehmen weiterhin von dieser akuten Problematik unberührt bleiben.



Sie haben Fragen? Wir freuen uns von Ihnen zu hören:
Telefon [+49 \(0\) 36967 / 595-0](tel:+490369675950) oder per E-Mail an support@datafox.de.

ANFRAGE STELLEN

Ihr Datafox Support Team

 [For our English speaking customers](#)

Dear Mr. Sippel,

You are using hardware from Datafox or have purchased devices from us in the past. For this reason, we would like to inform you that Datafox products (Datafox **hardware**, the Datafox **communication library** and **DatafoxStudioIV**) are **NOT** affected by the current Log4Shell/Log4j (CVE-2021-44228) vulnerability.



Info: Log4Shell (CVE-2021-44228)

What is the Log4Shell vulnerability?

In summary, the Log4Shell vulnerability is a computer or hardware vulnerability that hackers can target to gain unnoticed control or remote control over third-party devices. The German Federal Office for Security (BSI) classifies the Log4Shell vulnerability as particularly critical and has raised an already existing cyber security warning to the warning level RED.

As mentioned in the text above, Datafox products are NOT affected by this vulnerability. We hope that you and your company will remain unaffected by this acute issue.



Do you have suggestions for us or questions? We look forward to your feedback at any time and are happy to answer any questions you may have via phone +49 (0) 36967 / 595-0 or by e-mail: support@datafox.de.

Contact us!

Your Datafox Support Team



Datafox GmbH

Dermbacher Straße 12-14 - D-36419 Geisa

Telefon: +49 (0) 36967 / 595-0 Fax: -50

E-Mail: info@datafox.de

Internet: www.datafox.de

Geschäftsführer: Matthias Hartung, Markus Heil

Handelsregister Jena HRB500077 **UID:** DE812649245

Hinweis: Diese E-Mail geht ausschließlich an bestehende Kunden- bzw. Interessenten um Ihnen in unregelmäßigen Abständen Informationen zur Unterstützung Ihrer geschäftlichen Tätigkeit zu senden. Diesen E-Mail-Zusendungen haben Sie bisher nicht widersprochen. Daher gehen wir davon aus, dass Sie auch weiterhin Informationen auf elektronischem Wege erhalten wollen. Wenn Sie unseren Newsletter bzw. Produktinfo-Mailings nicht mehr erhalten möchten, dann klicken Sie auf [diesen Link](#).