

Wissen, wo es brennt - der Warn- und Informationsdienst VAS



AGENDA

- 1 Servicebeschreibung
- 2 Verfügbarkeit

Servicebeschreibung VAS – Vulnerability Advisory Service

A. Fitness (Prävention)	B. Monitoring	C. Notfall	D. Auswertung

- Kostenfreie Nutzung
- Zusammenarbeit mit der Deutsche Telekom Security GmbH
- aus über 2.000 Hard- und Softwareprodukten individuelle Liste zusammenstellbar
- individualisierte Schwachstellenwarnungen per E-Mail

<https://www.cert.sachsen.de/vulnerability-advisory-service.html>

Servicebeschreibung VAS – Vulnerability Advisory Service



**Vulnerability
Identified**



**Create
Advisory**



**Protected
Software**

ABLAUF

- Auswahl gewünschter Produkte über Weboberfläche → „Custom Advisory“ → „Produktliste“
(Anpassung jederzeit möglich)
- individuelle Warnmeldung bei Schwachstellen im Namen des SAX.CERT per E-Mail im PDF- oder XML-Format
- Bei fehlender Auswahl → alle neuen Schwachstellenmeldungen



sachsen.de ▾

Moderne Verwaltung ▾

E-Government ▾

» **SAX.CERT** ▾

- » Meldungen
- » Custom Advisory
- » Passwort
- » Abmelden

CERT-Meldungen

Risiko	Meldung	Datum	Status	Titel
	2023-0417	2023-02-27	new	Linux Kernel: Mehrere Schwachstellen
	2023-0416	2023-02-27	new	IBM MQ: Schwachstelle ermöglicht Denial of Service
	2023-0415	2023-02-27	new	Red Hat OpenShift: Schwachstelle ermöglicht Denial of Service
	2023-0414	2023-02-27	new	Zoho ManageEngine Endpoint Central: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen
	2023-0413	2023-02-27	new	Linux Kernel: Schwachstelle ermöglicht nicht spezifizierten Angriff
	2023-0412	2023-02-27	new	IBM SAN Volume Controller: Schwachstelle ermöglicht Privilegieneskalation
	2023-0411	2023-02-27	new	Linux Kernel: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff
	2023-0403	2023-02-27	update	Mono: Schwachstelle ermöglicht Codeausführung
	2023-0394	2023-02-27	update	Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff
	2023-0370	2023-02-27	update	Node.js: Mehrere Schwachstellen
	2023-0350	2023-02-27	update	ClamAV: Mehrere Schwachstellen
	2023-0333	2023-02-27	update	Intel Prozessoren: Mehrere Schwachstellen
	2023-0327	2023-02-27	update	PHP: Mehrere Schwachstellen

VAS – Web Oberfläche



VAS – Meldung via E-Mail

[SAX.CERT] Advisory-Meldedienst des SAX.CERT - Nachricht (HTML)

File | Nachricht | Nuance PDF | VIS | Was möchten Sie tun?

Ignorieren | Löschen | Antworten | Antworten und... | Verschieben in: ? | An Vorgesetzte(n) | Erledigt | Verschieben | Regeln | Als ungelesen markieren | Kategorisieren | Nachverfolgung | Übersetzen | Zoom

Mi 12.02.2020 13:38
SAX.CERT <dcert@dcert.de>
[SAX.CERT] Advisory-Meldedienst des SAX.CERT

An SID SAX.CERT

advisory_2020-0218.pdf 99 KB	advisory_2020-0217.pdf 96 KB	advisory_2020-0216.pdf 95 KB	advisory_2020-0215.pdf 93 KB	advisory_2020-0214.pdf 93 KB	advisory_2020-0213.pdf 93 KB
advisory_2020-0212.pdf 95 KB	advisory_2020-0211.pdf 104 KB	advisory_2020-0210.pdf 94 KB	advisory_2020-0209.pdf 94 KB	advisory_2020-0208.pdf 101 KB	advisory_2020-0207.pdf 96 KB
advisory_2020-0206.pdf	advisory_2020-0205.pdf	advisory_2020-0204.pdf	advisory_2020-0195.pdf	advisory_2020-0096.pdf	advisory_2019-1831.pdf

SecureMail Gateway des Freistaates Sachsen
Informationen zum Status dieser E-Mail:

- Die Nachricht war weder verschlüsselt noch digital unterschrieben.

Sehr geehrte SAX.CERT-Kunden,
heute erhalten Sie, entsprechend ihrer getroffenen Produktauswahl, folgende Meldungen:

Meldungsnummer	Titel	Bewertung (Angriffswahrscheinlichkeit / Schadenshöhe)
2020-0218	Mozilla Firefox und Thunderbird: Mehrere Schwachstellen	mittel / mittel-hoch
2020-0217	Adobe Acrobat und Reader: Mehrere Schwachstellen	mittel / mittel-hoch
2020-0216	Adobe Digital Editions: Mehrere Schwachstellen	mittel / mittel-hoch
2020-0215	Aruba Intelligent Edge Switches : Schwachstelle ermöglicht Offenlegung von Informationen	mittel / gering-mittel
2020-0214	Red Hat Quay: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen	gering-mittel / mittel-hoch

VAS – Meldung PDF

Advisory 2020-0211

Microsoft Windows: Mehrere Schwachstellen

Datum: 2020-02-12

Stand: 2020-02-12

Risiko gesamt

Angriffswahrscheinlichkeit: mittel-hoch

Potentielle Schadenshöhe: hoch

Plattformen

- Windows

betroffene Produkte

- Microsoft Windows 10
- Microsoft Windows 7 SP 1
- Microsoft Windows 8.1
- Microsoft Windows RT 8.1
- Microsoft Windows Server
- Microsoft Windows Server 2008 SP 2
- Microsoft Windows Server 2008 R2 SP 1

Verfügbarkeit

I Beantragung des Dienstes:

- E-Mail an **sax.cert@cert.sachsen.de**
- + mit **Betreff „dCERT“**
- + **Name** und **E-Mail-Adresse** des zukünftigen Nutzers
- SAX.CERT legt entsprechendes Konto an
- Nutzer erhält Zugangsdaten automatisch vom System

Erfahren Sie mehr...

Sie finden uns unter:
www.cert.sachsen.de

SAX.CERT

Staatsbetrieb Sächsische Informatik Dienste

Dresdner Str. 78 A

01445 Radebeul

Telefon (+49) 0351 79 99 77 99

E-Mail: sax.cert@cert.sachsen.de

