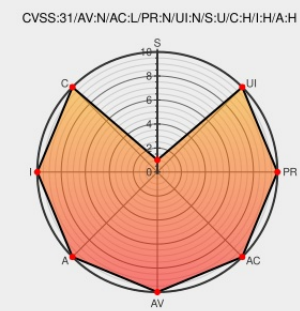
CVE-2022-36536

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2022-36536

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

An issue in the component post_applogin.php of Super Flexible Software GmbH & Co. KG Syncovery 9 for Linux v9.47x and below allows attackers to escalate privileges via creating crafted session tokens.

CVE-2022-36536 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
File Sync & Backup Software | The versatile all-in solution	syncovery.com text/html	MISC syncovery.com
Multiple vulnerabilities in Syncovery for Linux	www.mgm-sp.com text/html	MISC www.mgm-sp.com/en/multiple-vulnerabilities-in-syncovery-for-linux/
Copy of Универсальная страница компании	super.com text/html	MISC super.com

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Syncovery	Syncovery	All	All	All	All

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:

cpe:2.3:a:syncovery:syncovery:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-36536 : An issue in the component post_applogin.php of Super Flexible Software GmbH & Co. KG Syncovery 9 f… twitter.com/i/web/status/1…	2022-09-16 03:12:22
@Inceptus3	New Vulnerability: CVE-2022-36536 #InceptusSecure #UnderOurProtection	2022-09-16 05:13:17
/r/netcve	CVE-2022-36536	2022-09-16 04:39:08

← Previous ID

Next ID→