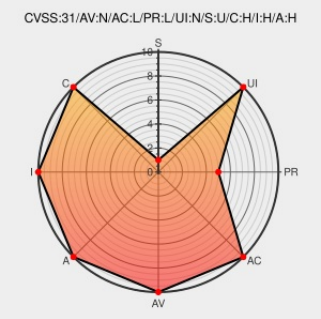
CVE-2023-32523

Published on: Not Yet Published

Last Modified on: 06/30/2023 06:27:00 PM UTC

CVE-2023-32523

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



Certain versions of Mobile Security from Trendmicro contain the following vulnerability:

Affected versions of Trend Micro Mobile Security (Enterprise) 9.8 SP5 contain some widgets that would allow a remote user to bypass authentication and potentially chain with other vulnerabilities. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit these vulnerabilities. This is similar to, but not identical to CVE-2023-32524.

CVE-2023-32523 has been assigned by security@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Trend Micro, Inc.** - **Trend Micro Moibile Security for Enterprise** version **< 9.8.3294**

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
DCX	success.trendmicro.com text/html	MISC success.trendmicro.com/dcx/s/solution/000293106?language=en_US
ZDI-23-587 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-23-587/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Mobile Security	9.8	sp5	All	All

cpe:2.3:a:trendmicro:mobile_security:9.8:sp5:*:*:enterprise:windows:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@TheZDIBugs	[ZDI-23-587|CVE-2023-32523] Trend Micro Mobile Security for Enterprises widget WFUser Authentication Bypass Vulnera… twitter.com/i/web/status/1…	2023-05-12 19:23:32
@CVEreport	CVE-2023-32523 : Affected versions of Trend Micro Mobile Security Enterprise 9.8 SP5 contain some widgets that wo… twitter.com/i/web/status/1…	2023-06-26 22:03:20

← Previous ID

Next ID→