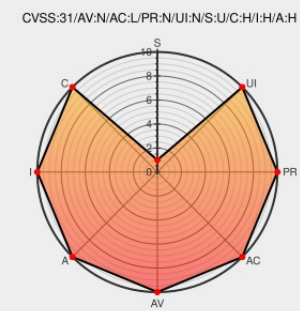
CVE-2023-26261

Published on: Not Yet Published

Last Modified on: 03/15/2023 01:43:00 PM UTC

CVE-2023-26261

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



Certain versions of Waap Cloud from Ubikasec contain the following vulnerability:

In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection leads to an authentication bypass by stealing the session of another connected user. The fixed versions are WAAP Gateway & Cloud 6.11.0 and 6.5.6-patch15.

CVE-2023-26261 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
CVE-2023-26261 - WAAP Gateway/Cloud - Authentication bypass via blind XPath injection · GitHub	gist.github.com text/html	MISC gist.github.com/Jakick/7d1635b886654ddd0e476b3c79a7ba9f
UBIKA	documentation.ubikasec.com text/html	MISC documentation.ubikasec.com/x/CQDAAw

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ubikasec	Waap Cloud	All	All	All	All
Application	Ubikasec	Waap Cloud	6.5.6	-	All	All
Application	Ubikasec	Waap Gateway	All	All	All	All
Application	Ubikasec	Waap Gateway	6.5.6	-	All	All

cpe:2.3:a:ubikasec:waap_cloud:*:*:*:*:*:*:*:*:

cpe:2.3:a:ubikasec:waap_cloud:6.5.6:-:*:*:*:*:*:*:

cpe:2.3:a:ubikasec:waap_gateway:*:*:*:*:*:*:*:*:

cpe:2.3:a:ubikasec:waap_gateway:6.5.6:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-26261 : In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection leads to an authentication bypas… twitter.com/i/web/status/1…	2023-03-08 15:04:30
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-26261 In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection… twitter.com/i/web/status/1…	2023-03-08 15:56:02
/r/netcve	CVE-2023-26261	2023-03-08 16:38:18

← Previous ID

Next ID→