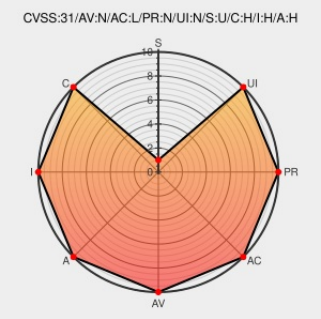
CVE-2022-37913

Published on: Not Yet Published

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

CVE-2022-37913

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



Certain versions of Aruba Edgeconnect Enterprise Orchestrator from Arubanetworks contain the following vulnerability:

Vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an unauthenticated remote attacker to bypass authentication. Successful exploitation of these vulnerabilities could allow an attacker to gain administrative privileges leading to a complete compromise of the Aruba EdgeConnect Enterprise Orchestrator with versions 9.1.2.40051 and below, 9.0.7.40108 and below, 8.10.23.40009 and below, and any older branches of Orchestrator not specifically mentioned.

CVE-2022-37913 has been assigned by security-alert@hpe.com 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
	www.arubanetworks.com text/plain	MISC www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-015.txt

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arubanetworks	Aruba Edgeconnect Enterprise Orchestrator	All	All	All	All
Application	Arubanetworks	Aruba Edgeconnect Enterprise Orchestrator	All	All	All	All
Application	Arubanetworks	Aruba Edgeconnect Enterprise Orchestrator	All	All	All	All
Application	Arubanetworks	Aruba Edgeconnect Enterprise Orchestrator	All	All	All	All

cpe:2.3:a:arubanetworks:aruba_edgeconnect_enterprise_orchestrator:*:*:*:*:as-a-service:*:*:*:

cpe:2.3:a:arubanetworks:aruba_edgeconnect_enterprise_orchestrator:*:*:*:*:global_enterprise_tenant_orchestrators:*:*:*:

cpe:2.3:a:arubanetworks:aruba_edgeconnect_enterprise_orchestrator:*:*:*:*:on-premises:*:*:*:

cpe:2.3:a:arubanetworks:aruba_edgeconnect_enterprise_orchestrator:*:*:*:*:sp:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@autumn_good_35	管理I/Fでの認証なしRCEなど。 ??? CVE: CVE-2022-37913, CVE-2022-37914, CVE-2022-37915 Severity: Critical Multiple Vulnerabilit… twitter.com/i/web/status/1…	2022-10-12 13:09:59
@EchelonEyes	Aruba исправила три критические уязвимости в EdgeConnect Orchestrator - CVE-2022-37913, CVE-2022-37914 и CVE-2022-3… twitter.com/i/web/status/1…	2022-10-13 11:47:03
@AWNetworks	Find Arctic Wolf's recommendations for CVE-2022-37913, CVE-2022-37914, CVE-2022-37915. ow.ly/xvp650LaEfo… twitter.com/i/web/status/1…	2022-10-14 19:07:25
@iototsecnews	Aruba EdgeConnect の深刻な脆弱性 CVE-2022-37913 などが FIX：認証バイパスの可能性 #security #vulnerability #aruba iototsecnews.jp/2022/10/13/aru…	2022-10-21 20:19:49
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-37913 Vulnerabilities in the web-based management interface of Aruba Ed… twitter.com/i/web/status/1…	2022-10-28 01:56:00
@CVEreport	CVE-2022-37913 : Vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator… twitter.com/i/web/status/1…	2022-10-28 02:04:40
/r/netcve	CVE-2022-37913	2022-10-28 03:38:52

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report