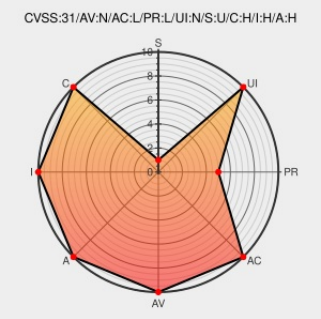
CVE-2022-43523

Published on: Not Yet Published

Last Modified on: 01/11/2023 03:44:00 PM UTC

CVE-2022-43523

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



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

Multiple vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the Aruba EdgeConnect Enterprise Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the Aruba EdgeConnect Enterprise Orchestrator host in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.

CVE-2022-43523 has been assigned by security-alert@hpe.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Hewlett Packard Enterprise (HPE)** - **Aruba EdgeConnect Enterprise Orchestration Software** version **= Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.**

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
	www.arubanetworks.com text/plain	MISC www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-021.txt

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Multiple vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could all…

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
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
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
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:*:*:*:

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:*:*:*:

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:*:*:*:

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)
@CVEreport	CVE-2022-43523 : Multiple vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orc… twitter.com/i/web/status/1…	2023-01-05 07:05:33
@vuldb	[Vuln] A severe vulnerability was disclosed for Aruba EdgeConnect Enterprise Orchestration (CVE-2022-43523) vuldb.com/?id.217463	2023-01-05 12:21:40
/r/netcve	CVE-2022-43523	2023-01-05 07:38:21

← Previous ID

Next ID→