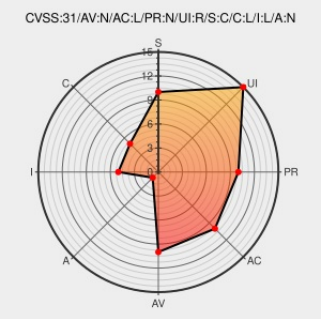
CVE-2022-43526

Published on: Not Yet Published

Last Modified on: 01/11/2023 03:42:00 AM UTC

CVE-2022-43526

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



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

Multiple vulnerabilities within the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface 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-2022-43526 has been assigned by security-alert@hpe.com to track the vulnerability - currently rated as MEDIUM 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: 6.1 - MEDIUM

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

CVE References

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

There are currently no QIDs associated with this CVE

Exploit/POC from Github

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

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-2022-43526 : Multiple vulnerabilities within the web-based management interface of Aruba EdgeConnect Enterprise… twitter.com/i/web/status/1…	2023-01-05 07:06:38
/r/netcve	CVE-2022-43526	2023-01-05 07:38:23

← Previous ID

Next ID→