From: advisory@cert-in.org.in
To: advisory <advisory@cert-in.org.in>
Date: 14 Oct 2022, 08:13:25 PM
Subject: [CIVN-2022-0395] Multiple Vulnerabilities in Aruba EdgeConnect Enterprise Orchestrator

Reply Reply To All Fwd Fwd As Attachment

HTML content follows

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Multiple Vulnerabilities in Aruba EdgeConnect Enterprise Orchestrator
Indian - Computer Emergency Response Team (cert-in.org.in)

Severity Rating: CRITICAL

Software Affected

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 9.1.2.40051 and prior
Orchestrator 9.0.7.40108 and prior
Orchestrator 8.10.23.40009 and prior
Any older branches of Orchestrator not specifically mentioned
Overview

Multiple vulnerabilities have been reported in Aruba EdgeConnect Enterprise Orchestrator which could allow a remote attacker to bypass security restrictions or conduct remote code execution attacks on the targeted system.

Description

1. Authentication Bypass Vulnerabilities (CVE-2022-37913 CVE-2022-37914)

These vulnerabilities exist in Aruba EdgeConnect Enterprise Orchestrator due to a flaw in the web-based management interface. A remote attacker could exploit these vulnerabilities to bypass security restrictions which leads to gaining administrative privileges.
Successful exploitation of these vulnerabilities could allow an attacker to completely compromise the Aruba EdgeConnect Enterprise Orchestrator host.

2. Remote Code Execution Vulnerability (CVE-2022-37915)

This vulnerability exists in Aruba EdgeConnect Enterprise Orchestrator due to command injection in the web-based management interface. An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary commands on the underlying host.
Successful exploitation of this vulnerability could allow an attacker to completely compromise the targeted system.

Workaround

Restrict CLI and web-based management interfaces to a dedicated layer 2 segment/VLAN and/or controlled by firewall policies at layer 3 and above.
Solution

Apply appropriate fix as mentioned in Aruba Network Security Advisory
https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-015.txt

Vendor Information

Aruba Network
https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-015.txt

References

Aruba Network
https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-015.txt

CVE Name
CVE-2022-37913
CVE-2022-37914
CVE-2022-37915

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE6r4Iam/Ey0c/KakL3jCgcSdcys8FAmNJdgsACgkQ3jCgcSdc
ys+Tuw//XtXfeHKQ4Ls/jxvvyIiuQn0KeKlrSvSxMHPrne2oiE20/7WJMMAexmbg
1T8+jbKWSRi3vNPfw9Q1qLbXImvSVT8Xk2soN4JlpNilFyj7MydXpV/B7aZmzUNB
9jmVGSqnFA4oG5ZdXZXQpDLIqUb8iK7Tp9oxGcKYVkayrX8Sy6RkMDjR0sQNX/GR
Gh5rPE6QxoRKYP7D52zUX/B4KjXkv2I6Eebga+PqWDmuAzItJEYUC7ibPi9a98ZS
NUtAKIFb651Y3BtUhxR779J/hXqdqy+HA0kG2XN6p1bi1thEdGGUhrT0VeYvWKt+
EvX7oL+kfi8CtlLJq7T2eBzeXig9fBRtG+wqrZ4t127EvlKZSTt92nbl6SiDjg+z
2OOp4XIovFdTtgFovp5kFZ7BIve/rhCqt6fsgkRJXMju5Gu48njwieUU+gsNEFk0
80awg30YOpp+7PaUxCyG3gV1D6ya2oN0w5m6WiIMJUBdiPlSe8diXRv985hs7/SD
oWX7KD3H2UeOuSxo0fmioIlTugvuogaCxHYFRP0YofBShCP8UFRZ/5OxL56HbbUj
37mKcx2FqrUdXxI/5Oh3Pv3csTCAL3MMmgI4p9Ol2n8LEGPOwHBAMkKJuS/XmRp8
ifcgOGVYTrfrNb0LJWlltzQGIn2vAMAHDdD/dNFwPoi1usbrB0s=
=AlO0
-----END PGP SIGNATURE-----