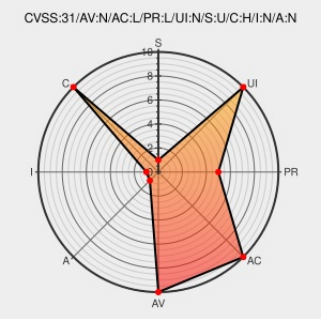
CVE-2020-3984

Published on: 11/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:39 PM UTC

CVE-2020-3984

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



Certain versions of Sd-wan Orchestrator from Vmware contain the following vulnerability:

The SD-WAN Orchestrator 3.3.2 prior to 3.3.2 P3 and 3.4.x prior to 3.4.4 does not apply correct input validation which allows for SQL-injection. An authenticated SD-WAN Orchestrator user may exploit a vulnerable API call using specially crafted SQL queries which may lead to unauthorized data access.

CVE-2020-3984 has been assigned by security@vmware.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
VMSA-2020-0025	Third Party Advisory www.vmware.com text/html	MISC www.vmware.com/security/advisories/VMSA-2020-0025.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Sd-wan Orchestrator	All	All	All	All
Application	Vmware	Sd-wan Orchestrator	3.3.2	-	All	All
Application	Vmware	Sd-wan Orchestrator	3.3.2	p1	All	All
Application	Vmware	Sd-wan Orchestrator	3.3.2	p2	All	All
Application	Vmware	Sd-wan Orchestrator	All	All	All	All
Application	Vmware	Sd-wan Orchestrator	3.3.2	-	All	All
Application	Vmware	Sd-wan Orchestrator	3.3.2	p1	All	All
Application	Vmware	Sd-wan Orchestrator	3.3.2	p2	All	All

cpe:2.3:a:vmware:sd-wan_orchestrator:*:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:sd-wan_orchestrator:3.3.2:-:*:*:*:*:*:*:

cpe:2.3:a:vmware:sd-wan_orchestrator:3.3.2:p1:*:*:*:*:*:*:

cpe:2.3:a:vmware:sd-wan_orchestrator:3.3.2:p2:*:*:*:*:*:*:

cpe:2.3:a:vmware:sd-wan_orchestrator:*:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:sd-wan_orchestrator:3.3.2:-:*:*:*:*:*:*:

cpe:2.3:a:vmware:sd-wan_orchestrator:3.3.2:p1:*:*:*:*:*:*:

cpe:2.3:a:vmware:sd-wan_orchestrator:3.3.2:p2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@ipssignatures	It's new to me that proofpoint has a protection/signature/rule for the vulnerability CVE-2020-3984.… twitter.com/i/web/status/1…	2022-02-05 02:02:00
@ipssignatures	It is the first time for me to know a protection/signature/rule for the vulnerability CVE-2020-3984. #Sgo34yv56egji6	2022-02-05 02:02:00

← Previous ID

Next ID→

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