NCSC
National Cyber Security Centre

2104081002-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Cisco SD-WAN vManage Software Vulnerabilities (CVE-2021-1137, CVE-2021-1479, CVE-2021-1480)

2021-04-08

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Threat Type	Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or allow an authenticated, local attacker to gain escalated privileges on an affected system. The full advisory from Cisco can be found here. • **CVE-2021-1479: Cisco SD-WAN vManage Remote Management Buffer Overflow Vulnerability (CVSS Base Score: 9.8)** – The vulnerability is due to improper validation of user-supplied input to the vulnerable component. An attacker could exploit this vulnerability by sending a crafted connection request to the vulnerable component that, when processed, could cause a buffer overflow condition. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. • **CVE-2021-1137: Cisco SD-WAN vManage Privilege Escalation Vulnerability (CVSS Base Score: 7.8)** – The vulnerability is due to insufficient input validation by the affected software. An authenticated attacker who has permissions to add new users or groups on the vManage system could exploit this vulnerability by modifying a user account. A successful exploit could allow the attacker to gain root privileges on the underlying operating system. • **CVE-2021-1480: Cisco SD-WAN vManage Privilege Escalation Vulnerability (CVSS Base Score: 7.8)** – The vulnerability is due to improper validation of input to the system file transfer functions. An authenticated attacker could exploit this vulnerability by sending specially crafted requests to the vulnerable system. A successful exploit could allow the attacker to overwrite arbitrary files and modify the system in such a way that could allow the attacker to gain root privileges on the underlying operating system.
Products Affected	These vulnerabilities affect Cisco devices if they are running a vulnerable release of Cisco SD-WAN vManage Software. For information about which Cisco software releases are vulnerable, see the Fixed Software section of the Cisco advisory.

Impact

- **CVE-2021-1479:** Could allow an unauthenticated, remote attacker to cause a buffer overflow condition.
- **CVE-2021-1137:** Could allow an authenticated, local attacker to gain escalated privileges on the underlying operating system.
- **CVE-2021-1480:** Could allow an authenticated, local attacker to gain escalated privileges on the underlying operating system.

Recommendations

Cisco has released software updates that address the vulnerabilities described in this advisory.

Fixed Releases:

Cisco SD-WAN vManage Release	First Fixed Release
18.4 and earlier	Migrate to a fixed release
19.2	19.2.4
19.3	Migrate to a fixed release
20.1	Migrate to a fixed release
20.3	20.3.3
20.4	20.4.1

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie