orangecertcc / **security-research** Public

Code   Pull requests   Actions   **Security** 35   Insights

Cisco IOx - Application Environment User Impersonation Vulnerability (CVE-2022-20724)

Moderate **orange-cert-cc** published **GHSA-xr7h-wjgg-h3rp** on Apr 19

Package

IOx (Cisco)

Affected versions	Patched versions
17.3.3	17.3(5)

Description

Overview

A vulnerability in the Cisco IOx application hosting environment of multiple Cisco platforms could allow an authenticated, remote attacker to read arbitrary files from the underlying host filesystem.

Impact

An attacker could exploit this vulnerability by sending a crafted command request using the API. A successful exploit could allow the attacker to read the contents of any file that is located on the host device filesystem.

Details

This vulnerability is due to insufficient path validation of command arguments within the Cisco IOx API.

Solution

Security patch

Upgrade to patched version (see above).

Workaround

There are no workarounds that address this vulnerability.

References

https://nvd.nist.gov/vuln/detail/CVE-2022-20724
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-yuXQ6hFj

Credits

Orange CERT-CC
Cyrille CHATRAS at Orange group

Timeline

Date reported: June 06, 2021
Date fixed: April 13, 2022

Severity

Moderate 5.3 / 10

CVSS base metrics

Attack vector	**Network**
Attack complexity	**High**
Privileges required	**None**
User interaction	**Required**
Scope	**Unchanged**
Confidentiality	**None**
Integrity	**High**
Availability	**None**

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N

CVE ID

CVE-2022-20724

Weaknesses

No CWEs