Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

A critical flaw in Cisco IOx Root Access Threat has been discovered

Date of Publication	Admiralty Code	TA Number
February 6, 2023	A1	TA2023063

Summary

First Seen: February **1**, 2023
Affected Product: Cisco IOS XE
Impact: A remote attacker execute arbitrary commands as root on the underlying host system of an affected device.

CVEs

CVE	NAME	PATCH
CVE-2023-20076	Command Injection Vulnerability in Cisco IOx Application	✓

Vulnerability Details

Cisco has released security updates to address a high-severity vulnerability in the Cisco IOx application hosting environment (CVE-2023-20076), which can be exploited to execute arbitrary commands as the root user on the underlying host operating system. The vulnerability is caused by inadequate sanitization of parameters used to activate a program. An attacker can take advantage of this flaw by deploying and activating an application in the Cisco IOx application hosting environment using a specially crafted activation payload file. The level of access provided by the flaw could permit the installation and concealment of backdoors. If an attacker takes advantage of this flaw, the malicious package will remain active until the device is factory reset or explicitly destroyed.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-20076	Cisco IOS XE 800 Series Industrial ISRs CGR1000 Compute Modules IC3000 Industrial Compute Gateways IR510 WPAN Industrial Routers	cpe:2.3:h:cisco_systems_Industrial_Integrated_Services_Routers:-:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	T1078 Valid Accounts	T1059 Command and Scripting Interpreter	T1098 Account Manipulation
T1203 Exploitation for Client Execution	T1068 Exploitation for Privilege Escalation	T1574 Hijack Execution Flow	

Patch Links

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL

References

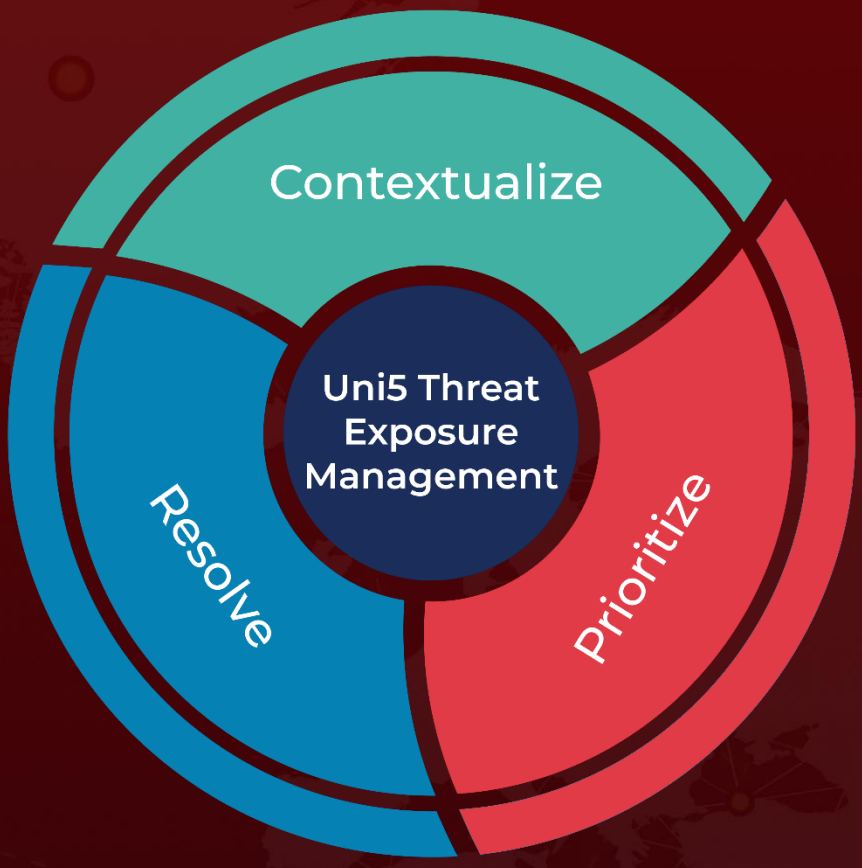
https://www.trellix.com/en-us/about/newsroom/stories/research/when-pwning-cisco-persistence-is-key-when-pwning-supply-chain-cisco-is-key.html

https://www.bleepingcomputer.com/news/security/cisco-fixes-bug-allowing-backdoor-persistence-between-reboots/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 6, 2023 • 5:30 AM

More at www.hivepro.com