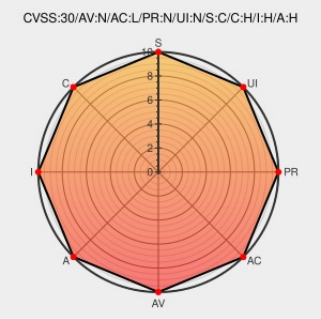
CVE-2020-6364

Published on: 10/14/2020 12:00:00 AM UTC

Last Modified on: 06/17/2021 05:22:00 PM UTC

CVE-2020-6364

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



Certain versions of Introscope Enterprise Manager from Sap contain the following vulnerability:

SAP Solution Manager and SAP Focused Run (update provided in WILY_INTRO_ENTERPRISE 9.7, 10.1, 10.5, 10.7), allows an attacker to modify a cookie in a way that OS commands can be executed and potentially gain control over the host running the CA Introscope Enterprise Manager,leading to Code Injection. With this, the attacker is able to read and modify all system files and also impact system availability.

CVE-2020-6364 has been assigned by cna@sap.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **SAP SE** - **SAP Solution Manager (CA Introscope Enterprise Manager) and SAP Focused Run (CA Introscope Enterprise Manager)** version **WILY_INTRO_ENTERPRISE 9.7**

Affected Vendor/Software: **SAP SE** - **SAP Solution Manager (CA Introscope Enterprise Manager) and SAP Focused Run (CA Introscope Enterprise Manager)** version **10.1**

Affected Vendor/Software: **SAP SE** - **SAP Solution Manager (CA Introscope Enterprise Manager) and SAP Focused Run (CA Introscope Enterprise Manager)** version **10.5**

Affected Vendor/Software: **SAP SE** - **SAP Solution Manager (CA Introscope Enterprise Manager) and SAP Focused Run (CA Introscope Enterprise Manager)** version **10.7**

CVSS3 Score: 10 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication

NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Full Disclosure: Onapsis Security Advisory 2021-0008: OS Command Injection in CA Introscope Enterprise Manager	seclists.org text/html	FULLDISC 20210614 Onapsis Security Advisory 2021-0008: OS Command Injection in CA Introscope Enterprise Manager
SAP Security Patch Day – October 2020 - Product Security Response at SAP - Community Wiki	Vendor Advisory wiki.scn.sap.com text/html	MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=558632196
SAP Wily Introscope Enterprise OS Command Injection ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/163153/SAP-Wily-Introscope-Enterprise-OS-Command-Injection.html
No Description Provided	Permissions Required launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2969828

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Remote code execution in CA APM Team Center (Wily Introscope)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Introscope Enterprise Manager	10.1	All	All	All
Application	Sap	Introscope Enterprise Manager	10.5	All	All	All
Application	Sap	Introscope Enterprise Manager	10.7	All	All	All
Application	Sap	Introscope Enterprise Manager	9.7	All	All	All
Application	Sap	Introscope Enterprise Manager	10.1	All	All	All
Application	Sap	Introscope Enterprise Manager	10.5	All	All	All
Application	Sap	Introscope Enterprise Manager	10.7	All	All	All
Application	Sap	Introscope Enterprise Manager	9.7	All	All	All

cpe:2.3:a:sap:introscope_enterprise_manager:10.1:*:*:*:*:*:*:*:

cpe:2.3:a:sap:introscope_enterprise_manager:10.5:*:*:*:*:*:*:*:

cpe:2.3:a:sap:introscope_enterprise_manager:10.7:*:*:*:*:*:*:*:

cpe:2.3:a:sap:introscope_enterprise_manager:9.7:*:*:*:*:*:*:*:

cpe:2.3:a:sap:introscope_enterprise_manager:10.1:*:*:*:*:*:*:*:

cpe:2.3:a:sap:introscope_enterprise_manager:10.5:*:*:*:*:*:*:*:

cpe:2.3:a:sap:introscope_enterprise_manager:10.7:*:*:*:*:*:*:*:

cpe:2.3:a:sap:introscope_enterprise_manager:9.7:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→