



CVE-2018-2399

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-2399
State	PUBLIC
Assigner	cna@sap.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-14 19:29:00 UTC
Updated	2019-10-09 23:40:00 UTC
Description	Cross-Site Scripting in Process Monitoring Infrastructure, from 7.10 to 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, due to inefficient e

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Process Monitoring Infrastructure	7.10	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.11	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.20	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.30	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.31	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.40	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.50	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.10	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.11	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.20	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.30	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.31	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.40	All	All	All
Application	Sap	Process Monitoring Infrastructure	7.50	All	All	All

References

Reference	Source	Link	Tags
-----------	--------	------	------

SAP Process Monitoring Infrastructure CVE-2018-2399 Cross Site Scripting Vulnerability	BID	www.securityfocus.com	Third F
launchpad.support.sap.com	CONFIRM	launchpad.support.sap.com	Permis
SAP Security Patch Day – March 2018 SAP Blogs	CONFIRM	blogs.sap.com	Vendor
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.