CVE-2019-0319

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-0319
State	PUBLIC
Assigner	cna@sap.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-10 19:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	The SAP Gateway, versions 7.5, 7.51, 7.52 and 7.53, allows an attacker to inject content which is displayed in the form of a

Risk And Classification

Problem Types: CWE-79 | CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Gateway	7.5	All	All	All
Application	Sap	Gateway	7.51	All	All	All
Application	Sap	Gateway	7.52	All	All	All
Application	Sap	Gateway	7.53	All	All	All
Application	Sap	Gateway	7.5	All	All	All
Application	Sap	Gateway	7.51	All	All	All
Application	Sap	Gateway	7.52	All	All	All
Application	Sap	Gateway	7.53	All	All	All
Application	Sap	Ui5	1.0.0	All	All	All
Application	Sap	Ui5	1.0.0	All	All	All

References

Reference	Source	Link	Ta
SAP UI5 1.0.0 is vulnerable to Content Spoofing in multiples parameters	MISC	cxsecurity.com	Thi
launchpad.support.sap.com	MISC	launchpad.support.sap.com	Pe
SAPUI5 1.0.0 / SAP Gateway 7.5 / 7.51 / 7.52 / 7.53 Content Spoofing ≈ Packet Storm	MISC	packetstormsecurity.com	Ex
SAP Gateway CVE-2019-0319 Content Injection Vulnerability	BID	www.securityfocus.com	Thi

launchpad.support.sap.com	MISC	launchpad.support.sap.com	
SAP Security Patch Day – July 2019 - Product Security Response at SAP - Community Wiki	CONFIRM	wiki.scn.sap.com	Ve
CVE-2019-0319.txt - Google Drive	MISC	drive.google.com	Ex
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

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