

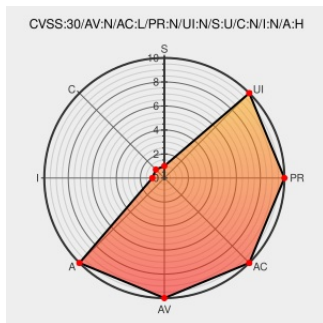


CVE-2018-2392

Published on: 02/14/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:52 PM UTC

CVE-2018-2392

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Internet Graphics Server](#) from [Sap](#) contain the following vulnerability:

Under certain conditions SAP Internet Graphics Server (IGS) 7.20, 7.20EXT, 7.45, 7.49, 7.53, fails to validate XML External Entity appropriately causing the SAP Internet Graphics Server (IGS) to become unavailable.

CVE-2018-2392 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Internet Graphics Server** version = 7.20

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Internet Graphics Server** version = 7.20EXT

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Internet Graphics Server** version = 7.45

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Internet Graphics Server** version = 7.49

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Internet Graphics Server** version = 7.53

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

NONE

PARTIAL

CVE References

Description	Tags	Link
No Description Provided	Permissions Required Vendor Advisory launchpad.support.sap.com text/html	 CONFIRM launchpad.support.sap.com/#/notes/2525222
SAP Security Patch Day – February 2018 SAP Blogs	Vendor Advisory blogs.sap.com text/html	 CONFIRM blogs.sap.com/2018/02/13/sap-security-patch-day-february-2018/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

SAP IGS XXE attack CVE-2018-2392 and CVE-2018-2393

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Internet Graphics Server	7.20	All	All	All
Application	Sap	Internet Graphics Server	7.20ext	All	All	All
Application	Sap	Internet Graphics Server	7.45	All	All	All
Application	Sap	Internet Graphics Server	7.49	All	All	All
Application	Sap	Internet Graphics Server	7.53	All	All	All
Application	Sap	Internet Graphics Server	7.20	All	All	All
Application	Sap	Internet Graphics Server	7.20ext	All	All	All
Application	Sap	Internet Graphics Server	7.45	All	All	All
Application	Sap	Internet Graphics Server	7.49	All	All	All
Application	Sap	Internet Graphics Server	7.53	All	All	All

cpe:2.3:a:sap:internet_graphics_server:7.20:*****:.*:

cpe:2.3:a:sap:internet_graphics_server:7.20ext:*****:.*:

cpe:2.3:a:sap:internet_graphics_server:7.45:*****:.*:

cpe:2.3:a:sap:internet_graphics_server:7.49:*****:.*:

cpe:2.3:a:sap:internet_graphics_server:7.53:*****:.*:

cpe:2.3:a:sap:internet_graphics_server:7.20:*****:*.:
cpe:2.3:a:sap:internet_graphics_server:7.20ext:*****:*.:
cpe:2.3:a:sap:internet_graphics_server:7.45:*****:*.:
cpe:2.3:a:sap:internet_graphics_server:7.49:*****:*.:
cpe:2.3:a:sap:internet_graphics_server:7.53:*****:*.:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →