



CVE-2020-12835

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

Summary

CVE	CVE-2020-12835
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-20 13:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	An issue was discovered in SmartBear ReadyAPI SoapUI Pro 3.2.5. Due to unsafe use of an Java RMI based protocol in a

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Smartbear	Readyapi	3.2.5	All	All	All
Application	Smartbear	Readyapi	3.2.5	All	All	All

References

Reference	Source	Link
Full Disclosure: [SYSS-2019-039] Smartbear ReadyAPI/SoapUI Pro/jProductivity Licensing Unsafe Deserialization	FULLDISC	seclists.org
www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-039.txt	MISC	www.syss.de
Pentest Blog – Aktuelle Themen rund um die SySS und ihre Arbeit	MISC	www.syss.de
Protection Licensing Toolkit ReadyAPI 3.2.5 Code Execution / Deserialization ≈ Packet Storm	MISC	packetstorm
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)