



CVE-2020-7980

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

Summary

CVE	CVE-2020-7980
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-25 19:15:00 UTC
Updated	2023-02-01 13:55:00 UTC
Description	Intellian Aptus Web 1.24 allows remote attackers to execute arbitrary OS commands via the Q field within JSON data to the

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Intelliantech	Aptus Web	1.24	All	All	All
Application	Intelliantech	Aptus Web	1.24	All	All	All

References

Reference	Source	Link
Satellian 1.12 Remote Code Execution ~ Packet Storm	MISC	packetstorm
GitHub - Xh4H/Satellian-CVE-2020-7980: PoC script that shows RCE vulnerability over Intellian Satellite controller	MISC	github.com
Skull Army: [Intellian] "Aptus Web" #RCE #Intellian (CVE-2020-7980)	MISC	sku11army.
CVE Program record	CVE.ORG	www.cve.or
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.

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