



CVE-2020-25247

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2020-25247
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-11 03:15:00 UTC
Updated	2022-12-06 21:30:00 UTC
Description	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. Directory traversal exists for v

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hyland	Onbase	All	All	All	All
Application	Hyland	Onbase	All	All	All	All

References

Reference	Source	Link	Tags
Full Disclosure: Hyland OnBase 19.x and below - Path Traversal	MISC	seclists.org	Mailing List, Third Party Advisory
Full Disclosure: Re: Navy Federal Reflective Cross Site Scripting (XSS)	FULLDISC	seclists.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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