



CVE-2020-3977

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

Summary

CVE	CVE-2020-3977
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-22 14:15:00 UTC
Updated	2020-09-30 17:20:00 UTC
Description	VMware Horizon DaaS (7.x and 8.x before 8.0.1 Update 1) contains a broken authentication vulnerability due to a flaw in th

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Horizon Daas	7.0.0	All	All	All
Application	Vmware	Horizon Daas	7.0.0	All	All	All
Application	Vmware	Horizon Daas	All	All	All	All

References

Reference	Source	Link	Tags
VMSA-2020-0021	MISC	www.vmware.com	Patch, Vendor Advisory
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.

Legacy QID Mappings

[373511](#) VMware Horizon DaaS Broken Authentication Vulnerability (VMSA-2020-0021)

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](#).

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