



CVE-2017-4897

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-4897
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-31 14:29:00 UTC
Updated	2017-07-17 13:18:00 UTC
Description	VMware Horizon DaaS before 7.0.0 contains a vulnerability that exists due to insufficient validation of data. An attacker may

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	VMware	Horizon Daas	All	All	All	All

References

Reference	Source
VMware Horizon DaaS Input Validation Flaw Lets Remote Users Access Devices and Drives on the Target System - SecurityTracker	SECT
VMSA-2017-0002	CONF
VMware Horizon DaaS CVE-2017-4897 Security Bypass Vulnerability	BID
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](#)