CVE-2017-4908

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-4908
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-08 13:29:00 UTC
Updated	2017-07-11 01:33:00 UTC
Description	VMware Workstation (12.x prior to 12.5.3) and Horizon View Client (4.x prior to 4.4.0) contain multiple heap buffer-overflow

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Horizon View	4.0	All	All	All
Application	Vmware	Horizon View	4.1	All	All	All
Application	Vmware	Horizon View	4.2	All	All	All
Application	Vmware	Horizon View	4.3	All	All	All
Application	Vmware	Horizon View	4.0	All	All	All
Application	Vmware	Horizon View	4.1	All	All	All
Application	Vmware	Horizon View	4.2	All	All	All
Application	Vmware	Horizon View	4.3	All	All	All
Application	Vmware	Workstation	12.0	All	All	All
Application	Vmware	Workstation	12.0.1	All	All	All
Application	Vmware	Workstation	12.1	All	All	All
Application	Vmware	Workstation	12.1.1	All	All	All
Application	Vmware	Workstation	12.5	All	All	All
Application	Vmware	Workstation	12.5.1	All	All	All
Application	Vmware	Workstation	12.5.2	All	All	All
Application	Vmware	Workstation	12.0	All	All	All
Application	Vmware	Workstation	12.0.1	All	All	All

Application	Vmware	Workstation	12.1	All	All	All
Application	Vmware	Workstation	12.1.1	All	All	All
Application	Vmware	Workstation	12.5	All	All	All
Application	Vmware	Workstation	12.5.1	All	All	All
Application	Vmware	Workstation	12.5.2	All	All	All

References

Reference
VMware Workstation and Horizon View Client CVE-2016-4908 Heap Based Buffer Overflow Vulnerability
VMware Horizon View Buffer Overflows Let Remote Users Execute Arbitrary Code and Guest Users Deny Service and Gain Elevated Privileg
VMware Workstation Heap Overflows Let Local Users on the Guest System Deny Service or Gain Elevated Privileges on the Host System - S
VMSA-2017-0008.2
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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