



CVE-2017-4933

Published on: 12/20/2017 12:00:00 AM UTC

Last Modified on: 02/03/2022 07:44:00 PM UTC

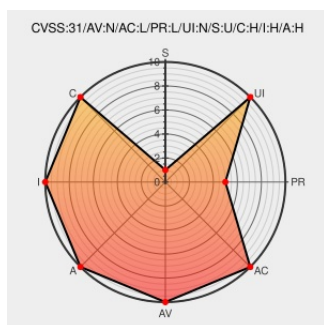
CVE-2017-4933

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Mac Os X](#) from [Apple](#) contain the following vulnerability:

VMware ESXi (6.5 before ESXi650-201710401-BG), Workstation (12.x before 12.5.8), and Fusion (8.x before 8.5.9) contain a vulnerability that could allow an authenticated VNC session to cause a heap overflow via a specific set of VNC packets resulting in heap corruption.

Successful exploitation of this issue could result in remote code execution in a virtual machine via the authenticated VNC session. Note: In order for exploitation to be possible in ESXi, VNC must be manually enabled in a virtual machine's .vmx configuration file. In addition, ESXi must be configured to allow VNC traffic through the built-in firewall.

CVE-2017-4933 has been assigned by [vmw](#) security@vmware.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [vmw](#) **VMware** - **ESXi** version **6.5 before ESXi650-201710401-BG**

Affected Vendor/Software: [vmw](#) **VMware** - **Workstation** version **12.x before 12.5.8**

Affected Vendor/Software: [vmw](#) **VMware** - **Fusion** version **8.x before 8.5.9**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact				
PARTIAL	PARTIAL	PARTIAL				
CVE References						
Description	Tags	Link				
VMware ESXi Buffer Overflows in Processing VNC Packets Let Remote Authenticated Users Execute Arbitrary Code and an Input Validation Flaw in the Host Client Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTrack 1040024				
VMSA-2017-0021	Issue Tracking Vendor Advisory www.vmware.com text/html	CONFIRM www.vmware.com/security/advisories/VMSA-2017-0021.html				
VMware Workstation and Fusion Buffer Overflows in Processing VNC Packets Let Remote Authenticated Users Execute Arbitrary Code - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTrack 1040025				
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.						
There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	-	All	All	All
Operating System	Vmware	Esxi	5.5	All	All	All
Operating System	Vmware	Esxi	6.0	All	All	All
Operating System	Vmware	Esxi	6.5	All	All	All
Operating System	Vmware	Esxi	6.5	-	All	All
Operating System	Vmware	Esxi	6.5	650-201701001	All	All
Operating System	Vmware	Esxi	6.5	650-201703001	All	All
Operating System	Vmware	Esxi	6.5	650-201703002	All	All
Operating System	Vmware	Esxi	6.5	650-201704001	All	All
Operating System	Vmware	Esxi	6.5	650-201707101	All	All

System						
Operating System	Vmware	Esxi	6.5	650-201707102	All	All
Operating System	Vmware	Esxi	6.5	650-201707103	All	All
Operating System	Vmware	Esxi	6.5	650-201707201	All	All
Operating System	Vmware	Esxi	6.5	650-201707202	All	All
Operating System	Vmware	Esxi	6.5	650-201707203	All	All
Operating System	Vmware	Esxi	6.5	650-201707204	All	All
Operating System	Vmware	Esxi	6.5	650-201707205	All	All
Operating System	Vmware	Esxi	6.5	650-201707206	All	All
Operating System	Vmware	Esxi	6.5	650-201707207	All	All
Operating System	Vmware	Esxi	6.5	650-201707208	All	All
Operating System	Vmware	Esxi	6.5	650-201707209	All	All
Operating System	Vmware	Esxi	6.5	650-201707210	All	All
Operating System	Vmware	Esxi	6.5	650-201707211	All	All
Operating System	Vmware	Esxi	6.5	650-201707212	All	All
Operating System	Vmware	Esxi	6.5	650-201707213	All	All
Operating System	Vmware	Esxi	6.5	650-201707214	All	All
Operating System	Vmware	Esxi	6.5	650-201707215	All	All
Operating System	Vmware	Esxi	6.5	650-201707216	All	All
Operating System	Vmware	Esxi	6.5	650-201707217	All	All
Operating System	Vmware	Esxi	6.5	650-201707218	All	All
Operating System	Vmware	Esxi	6.5	650-201707219	All	All
Operating System	Vmware	Esxi	6.5	650-201707220	All	All
Operating	Vmware	Esxi	6.5	650-201707221	All	All

System						
Operating System	Vmware	Esxi	6.5	650-201710001	All	All
Operating System	Vmware	Esxi	5.5	All	All	All
Operating System	Vmware	Esxi	6.0	All	All	All
Operating System	Vmware	Esxi	6.5	All	All	All
Application	Vmware	Fusion	All	All	All	All
Application	Vmware	Fusion	10.0	All	All	All
Application	Vmware	Fusion	10.1.0	All	All	All
Application	Vmware	Fusion	8.0.0	All	All	All
Application	Vmware	Fusion	8.0.1	All	All	All
Application	Vmware	Fusion	8.0.2	All	All	All
Application	Vmware	Fusion	8.1.0	All	All	All
Application	Vmware	Fusion	8.5.0	All	All	All
Application	Vmware	Fusion	8.5.1	All	All	All
Application	Vmware	Fusion	8.5.2	All	All	All
Application	Vmware	Fusion	8.5.3	All	All	All
Application	Vmware	Fusion	8.5.4	All	All	All
Application	Vmware	Fusion	8.5.5	All	All	All
Application	Vmware	Fusion	8.5.6	All	All	All
Application	Vmware	Fusion	8.5.7	All	All	All
Application	Vmware	Fusion	8.5.8	All	All	All
Application	Vmware	Fusion	10.0	All	All	All
Application	Vmware	Fusion	10.1.0	All	All	All
Application	Vmware	Fusion	8.0.0	All	All	All
Application	Vmware	Fusion	8.0.1	All	All	All
Application	Vmware	Fusion	8.0.2	All	All	All
Application	Vmware	Fusion	8.1.0	All	All	All
Application	Vmware	Fusion	8.5.0	All	All	All
Application	Vmware	Fusion	8.5.1	All	All	All
Application	Vmware	Fusion	8.5.2	All	All	All
Application	Vmware	Fusion	8.5.3	All	All	All
Application	Vmware	Fusion	8.5.4	All	All	All
Application	Vmware	Fusion	8.5.5	All	All	All
Application	Vmware	Fusion	8.5.6	All	All	All

Application	vmware	Fusion	8.5.0	All	All	All
Application	Vmware	Fusion	8.5.7	All	All	All
Application	Vmware	Fusion	8.5.8	All	All	All
Application	Vmware	Workstation Pro	All	All	All	All
Application	Vmware	Workstation Pro	12.0.0	All	All	All
Application	Vmware	Workstation Pro	12.0.1	All	All	All
Application	Vmware	Workstation Pro	12.1.0	All	All	All
Application	Vmware	Workstation Pro	12.1.1	All	All	All
Application	Vmware	Workstation Pro	12.5.0	All	All	All
Application	Vmware	Workstation Pro	12.5.1	All	All	All
Application	Vmware	Workstation Pro	12.5.2	All	All	All
Application	Vmware	Workstation Pro	12.5.3	All	All	All
Application	Vmware	Workstation Pro	12.5.4	All	All	All
Application	Vmware	Workstation Pro	12.5.5	All	All	All
Application	Vmware	Workstation Pro	12.5.6	All	All	All
Application	Vmware	Workstation Pro	12.5.7	All	All	All
Application	Vmware	Workstation Pro	14.0	All	All	All
Application	Vmware	Workstation Pro	14.1.0	All	All	All
Application	Vmware	Workstation Pro	12.0.0	All	All	All
Application	Vmware	Workstation Pro	12.0.1	All	All	All
Application	Vmware	Workstation Pro	12.1.0	All	All	All
Application	Vmware	Workstation Pro	12.1.1	All	All	All
Application	Vmware	Workstation Pro	12.5.0	All	All	All
Application	Vmware	Workstation Pro	12.5.1	All	All	All
Application	Vmware	Workstation Pro	12.5.2	All	All	All
Application	Vmware	Workstation Pro	12.5.3	All	All	All
Application	Vmware	Workstation Pro	12.5.4	All	All	All
Application	Vmware	Workstation Pro	12.5.5	All	All	All
Application	Vmware	Workstation Pro	12.5.6	All	All	All
Application	Vmware	Workstation Pro	12.5.7	All	All	All
Application	Vmware	Workstation Pro	14.0	All	All	All
Application	Vmware	Workstation Pro	14.1.0	All	All	All
cpe:2.3:o:apple:mac_os_x:-:*****:						
cpe:2.3:o:vmware:esxi:5.5:*****:						
cpe:2.3:o:vmware:esxi:6.0:*****:						

cpe:2.3:o:vmware:esxi:6.5:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:-:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201701001:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201703001:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201703002:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201704001:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707101:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707102:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707103:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707201:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707202:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707203:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707204:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707205:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707206:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707207:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707208:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707209:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707210:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707211:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707212:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707213:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707214:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707215:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707216:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707217:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707218:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707219:*:*:*:*:*:
cpe:2.3:o:vmware:esxi:6.5:650-201707220:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:6.5:650-201707220:*****:
cpe:2.3:o:vmware:esxi:6.5:650-201707221:*****:
cpe:2.3:o:vmware:esxi:6.5:650-201710001:*****:
cpe:2.3:o:vmware:esxi:5.5:*****:
cpe:2.3:o:vmware:esxi:6.0:*****:
cpe:2.3:o:vmware:esxi:6.5:*****:
cpe:2.3:a:vmware:fusion:*****:
cpe:2.3:a:vmware:fusion:10.0:*****:
cpe:2.3:a:vmware:fusion:10.1.0:*****:
cpe:2.3:a:vmware:fusion:8.0.0:*****:
cpe:2.3:a:vmware:fusion:8.0.1:*****:
cpe:2.3:a:vmware:fusion:8.0.2:*****:
cpe:2.3:a:vmware:fusion:8.1.0:*****:
cpe:2.3:a:vmware:fusion:8.5.0:*****:
cpe:2.3:a:vmware:fusion:8.5.1:*****:
cpe:2.3:a:vmware:fusion:8.5.2:*****:
cpe:2.3:a:vmware:fusion:8.5.3:*****:
cpe:2.3:a:vmware:fusion:8.5.4:*****:
cpe:2.3:a:vmware:fusion:8.5.5:*****:
cpe:2.3:a:vmware:fusion:8.5.6:*****:
cpe:2.3:a:vmware:fusion:8.5.7:*****:
cpe:2.3:a:vmware:fusion:8.5.8:*****:
cpe:2.3:a:vmware:fusion:10.0:*****:
cpe:2.3:a:vmware:fusion:10.1.0:*****:
cpe:2.3:a:vmware:fusion:8.0.0:*****:
cpe:2.3:a:vmware:fusion:8.0.1:*****:
cpe:2.3:a:vmware:fusion:8.0.2:*****:
cpe:2.3:a:vmware:fusion:8.1.0:*****:
cpe:2.3:a:vmware:fusion:8.5.0:*****:

```
cpe:2.3:a:vmware:fusion:8.5.1:*.:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:fusion:8.5.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:fusion:8.5.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:fusion:8.5.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:fusion:8.5.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:fusion:8.5.6:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:fusion:8.5.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:fusion:8.5.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.0.1:::*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.5.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.5.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.5.2:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:vmware:workstation_pro:12.5.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.5.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.5.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.5.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.5.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:14.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:14.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.0.1:::*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation_pro:12.1.1:*:*:*:*:*.*
```

```
cpe:2.3:a:vmware:workstation_pro:12.5.0:*:*:*:*:*:*
```

cpe:2.3:a:vmware:workstation_pro:12.5.1:*****:
cpe:2.3:a:vmware:workstation_pro:12.5.2:*****:
cpe:2.3:a:vmware:workstation_pro:12.5.3:*****:
cpe:2.3:a:vmware:workstation_pro:12.5.4:*****:
cpe:2.3:a:vmware:workstation_pro:12.5.5:*****:
cpe:2.3:a:vmware:workstation_pro:12.5.6:*****:
cpe:2.3:a:vmware:workstation_pro:12.5.7:*****:
cpe:2.3:a:vmware:workstation_pro:14.0:*****:
cpe:2.3:a:vmware:workstation_pro:14.1.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)