



CVE-2016-5333

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

Summary

CVE	CVE-2016-5333
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-31 01:59:00 UTC
Updated	2017-08-16 01:29:00 UTC
Description	VMware Photos OS OVA 1.0 before 2016-08-14 has a default SSH public key in an authorized_keys file, which allows remote users to access the target system.

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	VMware	Photon Os	All	2016-08-14	All	All

References

Reference	Source	Link
VMware Photon OS OVA CVE-2016-5333 Default Key Security Bypass Vulnerability	BID	www.securityfocus.com/bid/79833
VMSA-2016-0012	CONFIRM	www.vmware.com/security/vmsa-2016-0012
VMware shipped public key with its Photon OS-for-containers • The Register	MISC	www.theregister.com/2016/08/31/vmware_photon_os_ssh_key/
VMware Photon OS Default SSH Public Key Lets Remote Users Access the Target System - SecurityTracker	SECTRACK	www.securitytracker.com/id/1038444
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)