CVE-2014-1895

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-1895
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-01 06:35:00 UTC
Updated	2017-01-07 02:59:00 UTC
Description	Off-by-one error in the flask_security_avc_cachestats function in xsm/flask/flask_op.c in Xen 4.2.x and 4.3.x, when the max

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.3	All	All	All
Operating System	Xen	Xen	4.3.0	All	All	All
Operating System	Xen	Xen	4.3.1	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.3	All	All	All
Operating System	Xen	Xen	4.3.0	All	All	All
Operating System	Xen	Xen	4.3.1	All	All	All

References

Reference	Source	Link
oss-security - Re: Xen Security Advisory 84 - integer overflow in several XSM/Flask hypercalls	MLIST	www.ope
[security-announce] SUSE-SU-2014:0373-1: important: Security update for	SUSE	lists.oper

XSA-85 - Xen Security Advisories	CONFIRM	xenbits.x
Gentoo Linux Documentation -- Xen: Multiple Vunlerabilities	GENTOO	security.g
oss-security - Xen Security Advisory 85 (CVE-2014-1895) - Off-by-one error in FLASK_AVC_CACHESTAT hypercall	MLIST	www.ope
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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