



CVE-2010-1642

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

Summary

CVE	CVE-2010-1642
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-17 16:30:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The reply_sesssetup_and_X_spnego function in sesssetup.c in smbd in Samba before 3.4.8 and 3.5.x before 3.5.2 allows r

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samba	Samba	3.0.0	All	All	All

Application	Samba	Samba	3.0.1	All	All	All
Application	Samba	Samba	3.0.10	All	All	All
Application	Samba	Samba	3.0.11	All	All	All
Application	Samba	Samba	3.0.12	All	All	All
Application	Samba	Samba	3.0.13	All	All	All
Application	Samba	Samba	3.0.14	All	All	All
Application	Samba	Samba	3.0.14a	All	All	All
Application	Samba	Samba	3.0.15	All	All	All
Application	Samba	Samba	3.0.16	All	All	All
Application	Samba	Samba	3.0.17	All	All	All
Application	Samba	Samba	3.0.18	All	All	All
Application	Samba	Samba	3.0.19	All	All	All
Application	Samba	Samba	3.0.2	All	All	All
Application	Samba	Samba	3.0.20	All	All	All
Application	Samba	Samba	3.0.20a	All	All	All
Application	Samba	Samba	3.0.20b	All	All	All
Application	Samba	Samba	3.0.21	All	All	All
Application	Samba	Samba	3.0.21a	All	All	All
Application	Samba	Samba	3.0.21b	All	All	All
Application	Samba	Samba	3.0.21c	All	All	All
Application	Samba	Samba	3.0.22	All	All	All
Application	Samba	Samba	3.0.23	All	All	All
Application	Samba	Samba	3.0.23a	All	All	All
Application	Samba	Samba	3.0.23b	All	All	All
Application	Samba	Samba	3.0.23c	All	All	All
Application	Samba	Samba	3.0.23d	All	All	All
Application	Samba	Samba	3.0.24	All	All	All
Application	Samba	Samba	3.0.25	All	All	All
Application	Samba	Samba	3.0.25	pre1	All	All
Application	Samba	Samba	3.0.25	pre2	All	All
Application	Samba	Samba	3.0.25	rc1	All	All
Application	Samba	Samba	3.0.25	rc2	All	All
Application	Samba	Samba	3.0.25	rc3	All	All
Application	Samba	Samba	3.0.25a	All	All	All
Application	Samba	Samba	3.0.25b	All	All	All
Application	Samba	Samba	3.0.25c	All	All	All

Application	Samba	Samba	3.0.26	All	All	All
Application	Samba	Samba	3.0.26a	All	All	All
Application	Samba	Samba	3.0.27	All	All	All
Application	Samba	Samba	3.0.27a	All	All	All
Application	Samba	Samba	3.0.28	All	All	All
Application	Samba	Samba	3.0.28a	All	All	All
Application	Samba	Samba	3.0.29	All	All	All
Application	Samba	Samba	3.0.2a	All	All	All
Application	Samba	Samba	3.0.3	All	All	All
Application	Samba	Samba	3.0.30	All	All	All
Application	Samba	Samba	3.0.31	All	All	All
Application	Samba	Samba	3.0.32	All	All	All
Application	Samba	Samba	3.0.33	All	All	All
Application	Samba	Samba	3.0.34	All	All	All
Application	Samba	Samba	3.0.35	All	All	All
Application	Samba	Samba	3.0.36	All	All	All
Application	Samba	Samba	3.0.37	All	All	All
Application	Samba	Samba	3.0.4	All	All	All
Application	Samba	Samba	3.0.4	rc1	All	All
Application	Samba	Samba	3.0.5	All	All	All
Application	Samba	Samba	3.0.6	All	All	All
Application	Samba	Samba	3.0.7	All	All	All
Application	Samba	Samba	3.0.8	All	All	All
Application	Samba	Samba	3.0.9	All	All	All
Application	Samba	Samba	3.1.0	All	All	All
Application	Samba	Samba	3.2	All	All	All
Application	Samba	Samba	3.2.0	All	All	All
Application	Samba	Samba	3.2.1	All	All	All
Application	Samba	Samba	3.2.10	All	All	All
Application	Samba	Samba	3.2.11	All	All	All
Application	Samba	Samba	3.2.12	All	All	All
Application	Samba	Samba	3.2.13	All	All	All
Application	Samba	Samba	3.2.14	All	All	All
Application	Samba	Samba	3.2.15	All	All	All
Application	Samba	Samba	3.2.2	All	All	All

Application	Samba	Samba	3.2.3	All	All	All
Application	Samba	Samba	3.2.4	All	All	All
Application	Samba	Samba	3.2.5	All	All	All
Application	Samba	Samba	3.2.6	All	All	All
Application	Samba	Samba	3.2.7	All	All	All
Application	Samba	Samba	3.2.8	All	All	All
Application	Samba	Samba	3.2.9	All	All	All
Application	Samba	Samba	3.3	All	All	All
Application	Samba	Samba	3.3.0	All	All	All
Application	Samba	Samba	3.3.1	All	All	All
Application	Samba	Samba	3.3.10	All	All	All
Application	Samba	Samba	3.3.11	All	All	All
Application	Samba	Samba	3.3.2	All	All	All
Application	Samba	Samba	3.3.3	All	All	All
Application	Samba	Samba	3.3.4	All	All	All
Application	Samba	Samba	3.3.5	All	All	All
Application	Samba	Samba	3.3.6	All	All	All
Application	Samba	Samba	3.3.7	All	All	All
Application	Samba	Samba	3.3.8	All	All	All
Application	Samba	Samba	3.3.9	All	All	All
Application	Samba	Samba	3.4	All	All	All
Application	Samba	Samba	3.4.0	All	All	All
Application	Samba	Samba	3.4.1	All	All	All
Application	Samba	Samba	3.4.2	All	All	All
Application	Samba	Samba	3.4.3	All	All	All
Application	Samba	Samba	3.4.4	All	All	All
Application	Samba	Samba	3.4.5	All	All	All
Application	Samba	Samba	3.4.6	All	All	All
Application	Samba	Samba	3.5	All	All	All
Application	Samba	Samba	3.5.0	All	All	All
Application	Samba	Samba	3.5.1	All	All	All
Application	Samba	Samba	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version		Platforms	
CNA	Na	N/a	affected n/a		Not specified	

References	
Reference	Source
git.samba.org - samba.git/commit	af854a3a-2127-422
594921 – (CVE-2010-1635, CVE-2010-1642) CVE-2010-1635, CVE-2010-1642 samba: denial of service vulnerabilities	af854a3a-2127-422
Samba - Release Notes Archive	af854a3a-2127-422
Samba - Release Notes Archive	af854a3a-2127-422
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422
Samba Multiple Remote Denial of Service Vulnerabilities	af854a3a-2127-422
Support / Security / Advisories // MDVSA-2010:141 Mandriva	af854a3a-2127-422
Bug 7254 – An uninitialized variable read could cause an smbd crash.	af854a3a-2127-422
stratsec - Information security, consulting, intelligence and training	af854a3a-2127-422
CVE-2010-1642	af854a3a-2127-422
git.samba.org - samba.git/commit	MITRE
stratsec - Information security, consulting, intelligence and training	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
There are currently no legacy QID mappings associated with this CVE.	