CVE-2015-0528

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

Summary

CVE	CVE-2015-0528
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-29 10:59:00 UTC
Updated	2016-08-24 19:28:00 UTC
Description	The RPC daemon in EMC Isilon OneFS 6.5.x and 7.0.x before 7.0.2.13, 7.1.0 before 7.1.0.6, 7.1.1 before 7.1.1.2, and 7.2.(

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Emc	Isilon Onefs	7.1.0.0	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.1	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.2	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.3	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.4	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.5	All	All	All
Operating System	Emc	Isilon Onefs	7.1.1.0	All	All	All
Operating System	Emc	Isilon Onefs	7.1.1.1	All	All	All
Operating System	Emc	Isilon Onefs	7.2.0.0	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.0	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.1	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.2	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.3	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.4	All	All	All
Operating System	Emc	Isilon Onefs	7.1.0.5	All	All	All
Operating System	Emc	Isilon Onefs	7.1.1.0	All	All	All
Operating System	Emc	Isilon Onefs	7.1.1.1	All	All	All

Operating System	Emc	Isilon Onefs	7.2.0.0	All	All	All
Operating System	Emc	Isilon Onefs	All	All	All	All

References

Reference	Source	Link	Tags
EMC Isilon OneFS Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com	Third Party Advisory
Bugtraq: ESA-2015-049: EMC Isilon OneFS Privilege Escalation Vulnerability	BUGTRAQ	seclists.org	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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