CVE-2007-4361

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

Summary

CVE	CVE-2007-4361
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-08-15 19:17:00 UTC
Updated	2018-10-15 21:34:00 UTC
Description	NETGEAR (formerly Infrant) ReadyNAS RAIDiator before 4.00b2-p2-T1 beta creates a default SSH root password derived

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Readynas Raidiator	3.01c1-p1	All	All	All
Hardware	Netgear	Readynas Raidiator	3.01c1-p6	All	All	All
Hardware	Netgear	Readynas Raidiator	3.01c1-p1	All	All	All
Hardware	Netgear	Readynas Raidiator	3.01c1-p6	All	All	All

References

Reference	Source	Link	T
NETGEAR ReadyNAS RAIDiator Remote SSH Backdoor Vulnerability	BID	www.securityfocus.com	P
36357	OSVDB	www.osvdb.org	
infrant.com	CONFIRM	www.infrant.com	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
infrant.com	CONFIRM	www.infrant.com	
Infrant ReadyNAS Devices SSH Default Root Password Weakness - Advisories - Secunia	SECUNIA	secunia.com	P
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
NETGEAR ReadyNAS • View topic - SSH again	CONFIRM	www.infrant.com	
SecurityReason - Default Root Password in Infrant (now Netgear) ReadyNAS "RAIDiator"	SREASON	securityreason.com	
CVE Program record	CVE.ORG	www.cve.org	ca

NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**