503.276.7500 MAIN
503.223.0182 FAX

Tripwire, Inc | 101 SW Main Street, Suite 1500 | Portland, Oregon 97204 | USA

tripwire.com

Tripwire Security Advisory 2013-001:
NETGEAR ReadyNAS Complete System Takeover
Publication Date: 09/xx/2013
CVE-ID: CVE-2013-2751 (Command Injection), CVE-2013-2752 (XSRF)
IP360 Detection:
81891 "NETGEAR ReadyNAS FrontView Remote Command Execution"
Required ASPL Module: 522 Base

Vendor	Product	Component	Fixed Version
NETGEAR	ReadyNAS	FrontView web interface	4.2.x: 4.2.24 4.1.x: 4.1.12

Background

NETGEAR ReadyNAS is a network attached storage device with models marketed for both consumers and businesses. The ReadyNAS appliance uses an embedded Linux platform known as RAIDiator. RAIDiator includes an HTTP front-end application known as FrontView, which is used to configure file sharing and streaming over multiple protocols. ReadyNAS also offers users the option to create or download add-ons to provide features that are not included in the base RAIDiator firmware.

Impact Statement

Affected systems can be exploited to bypass all access controls revealing all data stored on the device and providing a possible foothold for launching further network attacks.

Vulnerability Description

The NETGEAR ReadyNAS RAIDiator firmware prior to the 4.2.24 release is prone to remote command execution through the FrontView web interface. An attacker can use an unauthenticated HTTP GET request to execute arbitrary commands as user 'admin' on the remote NAS device. This vulnerability exists due to a failure in /frontview/lib/np_handler.pl to sanitize user-input. (An eval is exposed as part of the 'forgot password' workflow.) This vulnerability can be exploited by an attacker on the local network or by a remote attacker using XSRF techniques. Due to various improper file system permissions, the admin user can execute commands as root.

Vendor Response

The vendor released RAIDiator firmware 4.2.24 and 4.1.12 to correct the command execution and other vulnerabilities reported over the previous year.

Tripwire Suggested Actions

1. Upgrade affected systems to the latest available firmware ASAP
2. Limit access to the ReadyNAS HTTP server as much as possible
3. Limit attack surface by disabling services which are not in use

Disclosure Timeline

4/8/2013	Initial vendor notification of FrontView command execution and XSRF
6/18/2013	Vendor is contacted again regarding a disclosure timeline
6/18/2013	Vendor acknowledges report and states that customers should move to their cloud service
7/13/2013	Vendor releases RAIDiator 4.2.24
7/19/2013	Researcher notified of RAIDiator 4.2.24 and 4.1.12 which fix 'many of the issues' reported
9/XX/2013	TSA-2013-001 is published

Credit: Craig Young, Tripwire VERT