ENCRIPTO®
InformationSecurity

Security Advisory

Netgear ProSafe Switches CVE-2013-4775 & CVE-2013-4776

21st of August 2013

Juan J. Güelfo
CEO, IT-security consultant and
IT-security researcher at Encripto AS

About Encripto AS

Encripto AS is a Norwegian company which provides specialized services in IT-security with superior quality. Our core expertise is education, security testing and security monitoring.

Encripto AS is committed to information security. We do research to discover trends, new vulnerabilities and better ways to mitigate them. We believe in acting as good internet citizens to the industry, whether you are a provider or a user.

You can read more about us at http://www.encripto.no

Timeline and revision history

- ***21st of August 2013***
  Coordinated disclosure.

- ***9th of August 2013***
  Mitigations recommended by the vendor.

- ***10th of July 2013***
  Issues acknowledged by the vendor.

- ***9th of July 2013***
  Vulnerability details disclosed to the vendor.

- ***6th of July 2013***
  Vulnerabilities discovered by the researcher.

Disclaimer

The material presented in this document is for educational purposes only. Encripto AS cannot be responsible for any loss or damage carried out by any technique presented in this material. The reader is the only one responsible for applying this knowledge, which is at his / her own risk.

Any of the trademarks, service marks, collective marks, design rights, personality rights or similar rights that are mentioned, used or cited in this document is property of their respective owners.

License

1. Background

According to the vendor, Netgear ProSafe is a cost-effective line of smart switches for Small and Medium Businesses (SMBs). The products cover an essential set of network features and easy-to-use web-based management. Power over Ethernet (PoE) and Stacking versions are also available.

2. Summary

A range of ProSafe switches are affected by two different vulnerabilities.

CVE-2013-4775: Unauthenticated startup-config disclosure.
CVE-2013-4776: Denial of Service vulnerability.

3. Affected products and software

CVE	Model	Firmware	Result
CVE-2013-4775	GS724Tv3 and GS716Tv2	5.4.1.13	**Vulnerable**
	GS724Tv3 and GS716Tv2	5.4.1.10	**Vulnerable**
	GS748Tv4	5.4.1.14	**Vulnerable**
	GS510TP	5.4.0.6	**Vulnerable**
	GS752TPS and GS728TPS	5.3.0.17	**Vulnerable**
	GS728TS and GS725TS	5.3.0.17	**Vulnerable**
	GS752TXS and GS728TXS	6.1.0.12	**Vulnerable**
CVE-2013-4776	GS724Tv3 and GS716Tv2	5.4.1.13	**Vulnerable (reboot)**
	GS724Tv3 and GS716Tv2	5.4.1.10	**Vulnerable (reboot)**
	GS748Tv4	5.4.1.14	**Vulnerable (crash)**
	GS510TP	5.0.4.4	**Vulnerable (reboot)**

4. Vulnerabilities

The list below describes the vulnerabilities discovered in the affected software.

- **CVE-2013-4775: Unauthenticated startup-config disclosure**
  The web management application fails to restrict URL access to different application areas. Remote, unauthenticated attackers could exploit this issue to download the device's startup-config, which contains administrator credentials in encrypted form.

  Proof of Concept
  The vulnerability can be exploited with a simple HTTP (GET) request.
  Open a browser and visit http://Target-IP/filesystem/startup-config

- **CVE-2013-4776: Denial of Service vulnerability**
  The affected products are prone to a Denial of Service vulnerability. Remote, unauthenticated attackers could exploit this issue to cause a switch reboot or crash, resulting in a loss of network connectivity for all devices connected to the switch.

  Proof of Concept
  The vulnerability can be exploited with a simple HTTP (GET) request.
  Open a browser and visit http://Target-IP/filesystem/

5. Remediation

No firmware updates or fixes have been released yet.
As a mitigation, the vendor recommends configuring a separate management VLAN and configure access control via “Security::Access::Access Control” or “Security::ACL::Advanced::IP Extended Rules”.

6. Credit

The vulnerabilities were originally discovered in a GS724Tv3 device, by Juan J. Güelfo at Encripto AS.
E-mail: post@encripto.no
Web: http://www.encripto.no

Special thanks to Maarten Hoogcarspel and the Netgear Support Team for verifying other switch models, and considering possible fixes.

For more information about Encripto’s research policy, please visit http://www.encripto.no/forskning/