MUST READ   A few hours the Paris attacks, a new ISIS propaganda hub appeared on

A flaw in D-Link Switches opens corporate networks to hack

November 17, 2015 By Pierluigi Paganini

A flaw in certain D-Link switches can be exploited by remote attackers to access configuration data and hack corporate networks.

The independent security researcher Varang Amin and the chief architect at Elastica's Cloud Threat Labs Aditya Sood have discovered a vulnerability in the D-Link Switches belonging to the DGS-1210 Series Gigabit Smart Switches.

The security experts revealed the existence of the flaw at the ToorCon security conference, but they avoided to disclose the details about the exploit to give the D-Link the necessary time to solve the issue.

This family of network devices allows the storage of backup files, including logs, firmware and configuration files, in the device's flash memory or on a web server. Unfortunately, the system lacks of proper authorization and authentication mechanisms, allowing an attacker to access the stored backup files.

The experts discovered that file stored in the flash memory can be accessed remotely by simply knowing the IP address of the D-Link Switches. The exposition of information contained in the configuration files could give the attackers precious information on the targeted network, the attackers could also control internal traffic by compromising the D-Link Switches.

"Once the configuration file is accessed, all the details about the switch, including configuration, username, etc., can be obtained by the attacker. For example, the configuration can be uploaded on another switch (purchased from the market) to obtain the details. Log files reveal information about the clients that accessed the switch and other infrastructure-related information," said Sood. *"Compromising network switches can have disastrous consequences as the attacker can control the traffic flow."*

The duo of experts highlighted that also the root directory of the web server is easily accessible by hackers.

"Usually, when the backup option is selected, the log files and configuration file are stored on the flash drive. Logs are enabled by default in many versions, but a majority of administrators have backup configured so downloading these files is easy," explained Sood.

Although the security vulnerability has been reported early October, D-Link hasn't fixed it yet.

Pierluigi Paganini

(**Security Affairs** – D-Link Switches, hacking)

Share it please ...

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".
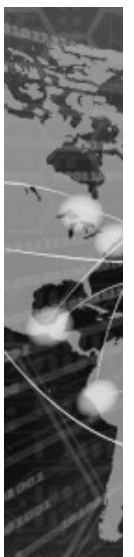
PREVIOUS ARTICLE

Stop DDoS attacks in seconds

MORE S

Stop DD

YOU MIGHT ALSO LIKE

An Israel
is trying
applicati
seconds.

Anonymous announced #OpParis against the ISIS in response to the Paris attacks

November 15, 2015 By Pierluigi Paganini

Stop DDoS attacks in seconds

November 17, 2015 By Pierluigi Paganini