#	Vulnerability groups according to IoT Inspector's report	Evaluation and response from Synology PSIRT
1	BusyBox CVE entries	Not exploitable remotely. Busybox is used only for internal services and is not exposed. Access is only possible if administrators enable SSH access.
2	curl CVE entries	Not exploitable remotely. The Curl library is used only by internal services and is not exposed. Access requires compromising and/or bypassing privilege checks, other applications, or system services.
3	GNU glibc CVE entries	Not exploitable remotely. GNU C Library (glibc) is used only by internal services. Access requires compromising and/or bypassing privilege checks, other applications, or system services. Relevant high-priority CVEs have mitigation applied.
4	GNU glibc getaddrinfo() buffer overflow	Already fixed in SRM 1.1 (2016)
5	Hardcoded password hashes	A predefined password is only used during the initial start-up process. The credentials are no longer valid after the user completes the device setup wizard. Additionally, "guest" accounts are disabled by default.
6	Linux Kernel CVE entries	Not exploitable remotely. Kernel-level vulnerabilities are only possible when bypassing or compromising multiple security features or privileged applications to exploit. Additionally, standard firewall rulesets will block WAN-initiated connections and access to most ports.
7	MiniUPnPd CVE entries	Not exploitable remotely. MiniUPnPd is utilized by internal services and is isolated from the WAN interface. The implementation used in SRM is not affected by the higher-severity CVE-2017-8798 (9.8).
8	OpenSSL CVE entries	False positive. The tool incorrectly determined the version implemented. The OpenSSL implementation used in the tested SRM version has all known CVEs mitigated as of this writing.
9	PHP CVE entries	Not exploitable remotely. PHP is utilized by internal services and is not exposed.
10	Samba CVE entries	Not exploitable remotely in regular use. By default SMB connections are disabled, and when enabled, default firewall rules will block external access.

#	Vulnerability groups according to IoT Inspector's report	Evaluation and response from Synology PSIRT
11	Avahi Daemon CVE entries	Not exploitable remotely in regular use. By default, the Avahi service is only allowed for LAN connections. Additionally, this vulnerability only results in the denial of service for the service provided by Avahi.
12	Dangerous service launch: Telnet	By default, Telnet is disabled and remains an option only for advanced users.
13	hostapd CVE entries	Not applicable. SRM does not use the affected hostapd TLS features. While not used, CVE-2019-16275 has been resolved as part of changes in SRM 1.2.4 and CVE-2021-30004 will be resolved as part of component upgrades in SRM 1.3.
14	Insecure OpenSSH Server Configuration: PermitRootLogin	By default, OpenSSH is disabled.
15	Insecure peer certificate/host-key verification	Not applicable. SRM does not use the unverified connection. This is deprecated code that has been left over and will be removed in a future update.
16	Insecure X.509 Certificates	The expired certificates are only used by SRM to initiate certain connections. These connections will typically fail unless specifically bypassed, as the endpoints will verify the connection by requiring valid certificates. These certificates will be updated in a future upgrade.
17	OpenSSH CVE entries	By default, OpenSSH is disabled.
18	Plaintext communication	Not applicable. Plaintext communication was identified in an unused section of code (commented out) and in a subsystem used only during the manufacturing process.
19	wpa_supplicant CVE entries	Not applicable. SRM does not use the affected Wi-Fi Direct and hostapd TLS functionality (#13)
20	Information leakage through DS_STORE files	Not a security concern. The file contains no information from the end-user or their device or network and is leftover from the development process. The redundant file will be removed in a future update.
21	Missing compile time mitigations on ELF binaries	Not a security vulnerability. Future updates will have this option enabled.
22	Unwanted software: tcpdump	Not a security vulnerability. tcpdump is used only for debugging purposes and is not exposed.

#	Vulnerability groups according to IoT Inspector's report	Evaluation and response from Synology PSIRT
23	Compliance and legal requirements	These items are informational and not security vulnerabilities.
24	Features extracted	
25	Images visualized	
26	Management protocol: UPnP (Universal Plug and Play)	
27	Management protocol: Wi-Fi Protected Setup (WPS)	
28	Private Keys	
29	Software component detection	
30	X.509 Certificates	