Technical Advisory: CVEs Assigned to Upstream Devices Exploited by Mirai IoT Botnet

Advisory #1

Product: All known XiongMai Technology Devices

Type of Device: IP Camera, DVR and NVR
Type of Vulnerability: Default Authentication w/ default service
Fix: None. Cannot disable service or change password
Remotely Exploitable: Yes
CVE ID:CVE-2016-1000245
Reporter: Flashpoint
Discover Date: 09/26/2016
Release Date: 10/06/2016

Summary:
All internet-capable XiongMai Technology boards running the DVR/NVR CMS (Also known as NetSurveillance) enable the telnet service to run on the primary ethernet interface. This service is run via /etc/rcS and cannot be disabled. The user "root" has a hardcoded and immutable password of xc3511. These systems do not have the "passwd" tool installed and the root password cannot be changed from command line nor from the web interface.

/etc $ cat passwd
root:absxcfbgXtb3o:0:0:root:/:/bin/sh
/etc $ cat passwd-
root:ab8nBoH3mb8.g:0:0::/root:/bin/sh

These systems are deployed in 124 countries around the world and the DVR, NVR and IP Camera parts manufactured by XM Technologies are sold white-labeled to downstream vendors. Unknown number of vendors utilize these products in their own branded solutions.

Affected Firmware:
All known firmware versions are affected, including the most recent release

Analysis of 20160924 Firmware:
root@localhost:~/_SimpGeneral_General_AHB7804R-MH-V2_V4.02.R11.7601.20160924.bin.extracted/_romfs-x.cramfs.img.extracted/squashfs-root/etc# cat passwd
root:absxcfbgXtb3o:0:0:root:/:/bin/sh
root@localhost:~/_SimpGeneral_General_AHB7804R-MH-V2_V4.02.R11.7601.20160924.bin.extracted/_romfs-x.cramfs.img.extracted/squashfs-root/etc# cat init.d/rcS | grep telnet
telnetd &
Matches password on DVR

Remediation:
Do not expose these devices directly to public internet access and contact your vendor for more information.

Advisory #2

Product: All internet capable XiongMai Technology Devices
Type of Device: IP Camera, DVR and NVR
Type of Vulnerability: Web Authentication Bypass
Fix: Not known
Remotely Exploitable: Yes
CVE ID: CVE-2016-1000246
Reporter: Flashpoint
Discover Date: 09/28/2016
Release Date: 10/06/2016

Summary:
Many known XiongMai DVRs, NVRs and IP Cameras run "CMS" (also called NetSurveillance) built by XM Technologies. This software is also used by all downstream vendors of XiongMai Technologies. The login page for these devices can be bypassed by simply changing the from http://<IP>/Login.htm to http://<IP>/DVR.htm. This allows you access to view all the camera systems without authentication. Furthermore, there is no logging on the system so user management is not possible. The web-server version on all affected products is the same; “uc-httpd”. All products currently affected by CVE-2016-1000245 are also vulnerable to the authentication bypass.

Affected Firmware:
All known firmware for all devices made by XiongMai Technology are vulnerable, including the 09/24/2016 release.

Remediation:
There is no fix currently. Best solution is to remove affected devices from public IPs and contact the manufacturer of your specific device.