08 Nov 2019

MINISTRY OF DEFENCE
CYBER CELL

CYBER SECURITY ADVISORY 12/2019
LARGE SCALE COMPROMISE OF SME/ SOHO ROUTER VIA EXPLOITING KNOWN VULNERABILITIES

1. It is learnt from reliable official source that a significant surge in compromise of routers deployed at SME sector and SOHO (Small Office and Home) segment is seen. Attackers behind these campaigns use some known variants of malware for targeting these IoT devices.

2. Some of the malware used by attackers in these attacks are Mirari, JenX, Satori IoT Botnet, Torii and Hajime Malware, etc. Recently, a surge in spreading an updated variant of malware JenX named as Gafgyt has been observed. The attacker behind these malware tries to exploit the known vulnerabilities present in Wi-Fi router deployed at SME Sector/ SOHO segment. The details of vulnerabilities along with router model targeted by attackers are provided below.

a) Command Injection Vulnerability (CVE-25017-18368). This vulnerability exists in Zyxel P660HN-T1A router. Successful exploitation of this vulnerability could result in unauthenticated user access thus resulting in disclosure of information.

b) Remote Code Execution Vulnerability (CVE-2017-17125) (CVE-2014-8361). This vulnerability exists in Huawei HG532 and Realtek RTL81XX chipset. Successful exploitation of this vulnerability leads to remote code execution on victim router.

3. Malicious Activity. Once the attacker successfully gains access of the router they can command the router to download binary using wget. Subsequently the binary runs on the infected router and tries to connect with the C2 controlled by attacker and register itself with attacker controlled botnet along with information like IP address, architecture details, etc. Finally the infected router becomes part of the attacker controlled botnet and starts performing different malicious activities based upon the commands it receives from C2 server. The IOC of attack are enumerated below.

Hashes

fb93601f8d4e0228276edff1c6fe635d
f1c099d65bf94e009f5e65238caac468

Command and Control server IP/ URL

185.172.110[.]224.993
185.172110[.]224/arm7
185.172.110[.]224/mips

4. Best Practice and Recommendations.

a) Restrict Web Management Interface access of IoT devices to authorized users only and change default username/ passwords.

b) Always change default login credentials before deployment in production. Change default credentials at device startup and ensure that passwords meet the maximum complexity.

c) Disable Universal Plug and Play (UPnP) on IoT devices unless absolutely required.

d) Users should be aware of the installed devices and their capabilities. If a device comes with a default password or an open Wi-Fi connection, users should change the password and only allow it tom operate on a home network with a secured Wi-Fi router.

e) Control access to the devices with access list and configure devices to “lock” or logout and require a user to re-authenticate if left unattended.

f) Identify systems with default passwords and implement above mentioned measures. Some of the systems that need to examine the Routers, switches, web applications and administrative web interfaces, ICS systems, Telnet and SSH interfaces.

g) Implement account lockout policies to reduce risk of brute forcing attacks.

j) Telnet and SSH should be disabled on device if there is no requirement of remote management.

k) Configure VPN and SSH to access device if there is no requirement of remote management.

l) Configure VPN and SSH to access device if remote access is required. And configure certificate based authentication for telnet client for remote management of devices.

m) Implement Egress and Ingress filtering at router level and report suspicious entries in routers to internet service provider.

n) Keep up-to-date Antivirus, patches and fixes on IoT devices, operating system and applications.

p) Unnecessary port and services should be stopped and closed. Logging must be enabled on the device to log all the activities.

q) Enable and monitor perimeter device logs to detect scan attempts towards critical devices/ systems.

5. The advisory may be disseminated to all concerned in the MoD. IT / EDP sections are advised to undertake patch management of affected systems accordingly.