***Final Report***

***Title: Securing IoT Devices: A Case Study on Home Automation***

***Authors***: *Sv. Deepthi, P. Teja Sri, P. Hemanath, K. Dushyanth, Lohith Naidu*

***1. Introduction***

In today’s digital age, Internet of Things (IoT) technology is revolutionizing homes through automation. However, these advancements come with substantial security risks. This report explores a critical vulnerability, known as CallStranger (CVE-2020-12695), found in the Universal Plug and Play (UPnP) protocol used in billions of IoT-enabled devices. By dissecting this vulnerability, we aim to understand its implications, spread awareness, and suggest effective mitigation strategies in the context of home automation systems.

2. Basic Concepts

• IoT (Internet of Things): A network of physical devices—including sensors, lights, thermostats, and other systems—that communicate and exchange data over the Internet.

• Cybersecurity: The practice of defending computers, servers, mobile devices, and networks from malicious attacks and unauthorized access.

• Home Automation: Technology that enables control over home features like lighting, climate, and security using smart devices and cloud-based systems.

3. Malware, Bugs & Threat Examples in IoT

• Malware Types Affecting IoT:

• Botnets: Mirai, Torii, Hajime—used to create large-scale DDoS attacks.

• Destructive Malware: Silex—designed to destroy IoT devices.

• Rootkits: Malicious software that hides deeper within a system, enabling continued intrusion.

• Bugs: Software vulnerabilities that can be exploited—like CallStranger being exploited via malformed UPnP messages.

4. Case Study: CallStranger Vulnerability (CVE-2020-12695)

Overview:

Discovered by security researcher Yunus Çadırcı, CallStranger highlights a severe flaw in the UPnP protocol that could enable attackers to:

• Exfiltrate data.

• Bypass firewalls with internal scanning.

• Launch large-scale amplified DDoS (Distributed Denial-of-Service) attacks.

Root Cause:

The vulnerability exists in improper validation of the Callback header in UPnP SUBSCRIBE requests. This allows arbitrary URLs to be inserted, causing targeted devices to send requests to malicious endpoints.

Affected Protocol:

• Universal Plug and Play (UPnP): A protocol designed for easy device discovery and communication within LAN networks, now misused due to security flaws.

5. Attack Flow & Consequences

Attack Methodology:

1. A malicious SUBSCRIBE request is sent with a forged Callback header.

2. The UPnP-enabled IoT device unknowingly sends a request to an attacker-controlled server.

3. Based on the setup, attackers can use this to:

• Conduct Server-Side Request Forgery (SSRF).

• Bypass NAT and firewall protections.

• Cause data exfiltration from secure internal networks.

• Launch amplified DDoS attacks using the victim device.

Severity:

• CVSS v3.1 Score: 7.5 (High)

• No user interaction or privileged access is required.

• Affects billions of devices globally including:

• Smart TVs

• Routers

• Consoles

• IP Cameras

• Printers

• Home Hubs

6. Detection and Scope

Detection Tools & Indicators:

• Security platforms like Zeek can detect exploit signatures.

• Custom scripts (e.g., on GitHub by the vulnerability’s discoverer) verify vulnerable endpoints.

• Monitoring for unusual UPnP SUBSCRIBE and NOTIFY traffic is essential.

Scope of Affected Devices:

• Popular vendors: Cisco, D-Link, Huawei, Netgear, TP-Link, Zyxel, and many more.

• Operating Systems: Windows 10, Xbox, embedded firmware in devices.

7. Real-World Risks and Impacts

• Risks:

• Information leakage and internal scanning.

• Disruption of Smart Home systems.

• Potential loss of personal/private information.

• Network instability due to unintended DDoS amplification.

• Long-Term Implications:

• A large number of devices remain unpatched.

• The flaw exposes weaknesses in default open configurations in many IoT ecosystems.

• It raises awareness of the danger of insecure UPnP implementations.

8. Mitigation Techniques

Recommended Actions:

• Disable UPnP on all devices that do not strictly need it—especially those exposed to the internet.

• Apply firmware and software patches provided by manufacturers.

• Introduce firewall rules to block external UPnP traffic (port 1900 UDP).

• Use network segmentation to isolate IoT devices.

• Monitor networks for abnormal UPnP traffic using tools like Wireshark.

Update by OCF:

• On April 17, 2020, the Open Connectivity Foundation (OCF) released an updated UPnP specification with mitigations and stricter validation logic.

9. Key Takeaways & Conclusion

• CallStranger demonstrates how a seemingly minor flaw in a widely-used protocol can lead to widespread IoT exposure.

• Securing IoT devices requires continuous updates, protocol hardening, and secure network designs.

• As home automation systems grow in popularity, users and manufacturers must take proactive security measures to limit exposure.

• Long-term, there is a strong need for:

• Better device-level security standards.

• Robust vendor accountability.

• Increased public and developer awareness on protocol vulnerabilities.

10. References

1. CVE-2020-12695 – NIST National Vulnerability Database

2. CallStranger Official Advisory: https://callstranger.com

3. OCF UPnP Specification Update – April 2020

4. Zeek Blog – CallStranger Detection Techniques

5. Yunus Çadırcı GitHub – CallStranger Checker Scripts.