Abstract – This document provides an in-depth analysis of the threats posed by malicious cyber actors exploiting insecure Small Office/Home Office (SOHO) routers. The analysis covers various aspects, including Security Defects and Exploits, Impact on Critical Infrastructure, Secure by Design Principles, Vulnerability and Exposure Research.

The document offers a qualitative summary of the current state of SOHO router security, highlighting the risks posed by insecure devices and the steps that can be taken to mitigate these risks. The analysis is beneficial for security professionals, manufacturers, and various industry sectors, providing a comprehensive understanding of the threats and guiding principles for enhancing the security of SOHO routers.

I. Introduction

The exploitation of insecure SOHO routers by malicious cyber actors, particularly state-sponsored groups, poses a significant threat to individual users and critical infrastructure. Manufacturers are urged to adopt secure by design principles and transparency practices to mitigate these risks, while users and network defenders are advised to implement best practices for router security and remain vigilant against potential threats.

II. Root of Insecure SOHO Routers

The root causes of insecure SOHO routers are multifaceted, involving both technical vulnerabilities and lapses in secure design and development practices by manufacturers, as well as negligence on the part of users in maintaining router security.

- **Widespread Vulnerabilities**: A significant number of vulnerabilities, totaling 226, have been identified in popular SOHO router brands. These vulnerabilities range in severity but collectively pose a substantial security risk.
- **Outdated Components**: Core components such as the Linux kernel and additional services like VPN in these routers are outdated. This makes them susceptible to known exploits for vulnerabilities that have long since been made public.
- **Insecure Default Settings**: Many routers come with easy-to-guess default passwords and use unencrypted connections. This can be easily exploited by attackers.
- **Lack of Secure Design and Development**: SOHO routers often lack basic security features due to insecure design and development practices. This includes the absence of automatic update capabilities and the presence of exploitable defects, particularly in web management interfaces.
- **Exposure of Management Interfaces**: Manufacturers frequently create devices with management interfaces exposed to the public internet by default, often without notifying the customers of this frequently unsafe configuration.
- **Lack of Transparency and Accountability**: There is a need for manufacturers to embrace transparency by disclosing product vulnerabilities through the CVE program and accurately classifying these vulnerabilities using the Common Weakness Enumeration (CWE) system
- **Neglect of Security in Favor of Convenience and Features**: Manufacturers prioritize ease of use and a wide variety of features over security, leading to routers that are "secure enough" right out of the box without considering the potential for exploitation.
- **User Negligence**: Many users, including IT professionals, do not follow basic security practices such as changing default passwords or updating firmware, leaving routers exposed to attacks.
- **Complexity in Identifying Vulnerable Devices**: Identifying specific vulnerable devices is complex due to legal and technical issues, complicating the process of mitigating these vulnerabilities.

III. Affected Industries

The exploitation of insecure SOHO routers poses a significant threat across multiple sectors, highlighting the need for improved security practices and awareness.

A. Communications

- **Data Breaches and Eavesdropping**: Insecure routers can lead to unauthorized access to network traffic, allowing attackers to intercept sensitive communications.
- **Disruption of Services**: Compromised routers can be used to launch Distributed Denial of Service (DDoS) attacks, disrupting communication services.

B. Transportation

Infrastructure Vulnerability: The transportation sector relies heavily on networked systems for operations. Compromised routers could allow attackers to disrupt traffic management systems and logistics operations.

C. Water

Operational Technology (OT) Threats: Insecure routers can provide a gateway for attackers to target OT systems within

the water sector, potentially affecting water treatment and distribution systems.

D. Energy

Grid Security: The energy sector, particularly electric utilities, is at risk of targeted attacks through insecure routers. Attackers could gain access to control systems, posing a threat to the stability of the power grid.

E. Other Industries

- **Healthcare**: Insecure routers can compromise patient data and disrupt medical services by providing attackers access to healthcare networks.
- **Retail and Hospitality**: These sectors are vulnerable to data breaches involving customer information and financial transactions due to insecure network devices.
- **Manufacturing**: Industrial control systems can be compromised through insecure routers, affecting production lines and industrial processes.
- **Education**: Schools and universities are at risk of data breaches and disruption of educational services.
- **Government and Public Sector**: Insecure routers can lead to unauthorized access to government networks, risking sensitive information and critical services

IV. Key Findings on Malicious Cyber Actors Exploiting Insecure SOHO Routers

- **Exploitation by State-Sponsored Groups**: The People's Republic of China (PRC)-sponsored Volt Typhoon group is actively compromising SOHO routers by exploiting software defects. These compromised routers are then used as launching pads to further compromise U.S. critical infrastructure entities.
- **Impact on Critical Infrastructure**: Compromised SOHO routers pose a significant threat as they can be used to move laterally within networks and further compromise critical infrastructure sectors in the U.S., including communications, energy, transportation, and water sectors.
- **ZuoRAT Campaign**: A sophisticated campaign leveraging infected SOHO routers, dubbed ZuoRAT, has been identified. This campaign involves a multistage remote access trojan (RAT) developed for SOHO devices, enabling attackers to maintain a low-detection presence on target networks and exploit sensitive information.
- **FBI's Response to Chinese Malware**: The FBI has taken proactive measures to disrupt the activities of Chinese hackers, specifically targeting SOHO routers infected with the KV Botnet malware. This involved issuing covert commands to infected devices to remove the malware and prevent further access by the hackers, highlighting the ongoing efforts to counteract the threats posed by compromised SOHO routers.

A. Tactics and Techniques

- **KV Botnet Malware**: Volt Typhoon actors have implanted KV Botnet malware into end-of-life Cisco and NETGEAR SOHO routers, which are no longer supported with security patches or software updates.
- **Concealment of Origin**: By routing their malicious activities through SOHO routers, these actors can conceal the PRC origin of their hacking activities, making it more challenging to detect and attribute the attacks.
- **Targeting Personal Emails**: Volt Typhoon actors have been observed targeting the personal emails of key network and IT staff to gain initial access to networks.
- **Use of Multi-Hop Proxies**: For command and control (C2) infrastructure, the actors use multi-hop proxies typically composed of virtual private servers (VPSs) or SOHO routers.
- **Living Off the Land (LOTL) Techniques**: Instead of relying on malware for post-compromise execution, Volt Typhoon actors use hands-on-keyboard activity via command-line and other native tools and processes on systems, a strategy known as LOTL, to maintain and expand access to victim networks.
- **Man-in-the-Middle Attacks**: Attackers can exploit vulnerabilities in routers to intercept and manipulate data passing through the network, leading to data breaches, identity theft, and espionage.
- **Gateway to Further Exploitation**: Once compromised, a router can serve as a gateway for attackers to launch further attacks on connected devices, including computers, smartphones, and smart home devices.
- **Botnet Recruitment**: Insecure routers can be easily compromised and recruited into botnets, large networks of infected devices used to launch distributed denial-of-service (DDoS) attacks, spam campaigns, and other malicious activities.

B. Impact and Response

- **Public-Private Partnerships**: The response to the Volt Typhoon compromises involved close collaboration between government agencies, including the FBI and CISA, and private sector entities. This partnership facilitated the sharing of threat intelligence, technical indicators of compromise (IoCs), and best practices for mitigation.
- **Firmware Analysis and Patching**: Manufacturers of affected SOHO routers were alerted to the vulnerabilities being exploited by Volt Typhoon actors. Efforts were made to analyze the malicious firmware, understand the exploitation techniques, and develop patches to address the vulnerabilities.
- **Disruption Operations**: Law enforcement and cybersecurity agencies undertook operations to disrupt the Volt Typhoon campaign. This included identifying and taking down C2 servers, removing malicious firmware from compromised routers, and blocking traffic to known malicious IP addresses.
- **Global Notification and Mitigation Campaign**: A global campaign was launched to notify owners of compromised SOHO routers and provide them with guidance on mitigating the threat. This included

instructions for resetting devices to factory settings, updating firmware, and changing default passwords.

- **Disruption of Critical Infrastructure**: The exploitation of these routers poses a significant threat as it could potentially disrupt essential services provided by critical infrastructure sectors.
- **Federal Response**: The FBI and the Justice Department have conducted operations to disrupt the KV Botnet by remotely deleting the malware from infected routers and taking steps to sever their connection to the botnet.
- **Mitigation Efforts**: The FBI has been notifying owners or operators of SOHO routers that were accessed during the takedown operation. The mitigation steps authorized by the court are temporary, and a router restart without proper mitigation will leave the device vulnerable to reinfection.
- **Secure by Design**: CISA and the FBI urge SOHO router manufacturers to build security into the design, development, and maintenance of SOHO routers to eliminate the paths these threat actors take to compromise devices and critical infrastructure entities.
- **Transparency and Disclosure**: Manufacturers are encouraged to protect against Volt Typhoon activity and other cyber threats by disclosing vulnerabilities through the CVE program and accurately classifying them using the CWE system.
- **User Vigilance**: Device operators are advised to update software, harden configurations, and add security solutions where necessary to combat threats

C. *Public and Customer Demand for Security*

In today's digital age, the security of network devices has become a paramount concern for both the public and businesses alike. This heightened awareness stems from an increasing number of high-profile cyberattacks and data breaches, which have underscored the vulnerabilities inherent in connected devices. As a result, there is a growing demand from customers and the public for manufacturers to prioritize security in their products.

1) *Factors Driving Demand*

- **Increased Awareness of Cyber Threats**: The general public and businesses are becoming more aware of the risks associated with cyber threats, including the potential for financial loss, privacy breaches, and disruption of services.
- **Regulatory Pressure**: Governments and regulatory bodies worldwide are implementing stricter regulations and standards for cybersecurity, compelling manufacturers to enhance the security features of their products.
- **Economic Impact of Cyberattacks**: The economic repercussions of cyberattacks, including the cost of recovery and the impact on brand reputation, have made security a critical consideration for customers when selecting products.
- **Interconnectedness of Devices**: The proliferation of IoT devices and the interconnectedness of digital ecosystems have amplified the potential impact of compromised devices, making security a top priority for ensuring the integrity of personal and corporate data.

2) *Customer Expectations*

- **Built-in Security Features**: Customers now expect devices to come with robust, built-in security features that protect against a wide range of threats without requiring extensive technical knowledge to configure.
- **Regular Security Updates**: There is an expectation for manufacturers to provide regular and timely security updates to address new vulnerabilities as they are discovered.
- **Transparency**: Customers demand transparency from manufacturers regarding the security of their products, including clear information about known vulnerabilities and the steps being taken to address them.
- **Ease of Use**: While demanding high levels of security, customers also expect these features to be user-friendly and not to impede

D. *Manufacturer Responsibility*

1) *Core Elements of Secure by Design*

- **Security as a Foundational Requirement**: Security must be considered a primary requirement, akin to functionality, usability, and performance. This means integrating security considerations into the product design, development lifecycle, and architectural decisions.
- **Minimization of Attack Surfaces**: Reducing the number of potential points of attack within a system that involves limiting the functionality and access rights of the system to only what is necessary for its operation.
- **Default Secure Settings**: Products should ship with secure settings by default, requiring users to make conscious decisions to weaken security. This includes strong default passwords, disabled unnecessary services, and enabled encryption.
- **Principle of Least Privilege**: Ensuring that processes, users, and systems operate using the minimum set of privileges necessary to perform their tasks. This limits the potential damage from an exploit or breach.
- **Secure Failure:** Designing systems to fail securely in the event of a compromise. This means that when a system encounters an error or breach, it defaults to a state that minimizes risk and exposure.
- **Security Through Transparency**: Encouraging openness about the design and implementation of security features, allowing for public scrutiny and peer review. This transparency helps identify and rectify vulnerabilities more effectively.
- **Privacy by Design**: Integrating privacy considerations into product development, ensuring that user data is protected and handled responsibly.

2) *Implementing Secure by Design in SOHO Routers*

- **Automatic Updates**: Implementing mechanisms for automatic firmware updates to ensure that routers are always running the latest version with the most recent security patches. This reduces the reliance on users to manually update their devices.
- **Digital Signing**: Ensuring that updates are digitally signed to verify their authenticity and integrity. This prevents the installation of malicious firmware updates that could compromise the router.
- **Secure Web Management Interface**: Placing the web management interface on LAN-side ports and improving its security to allow safe usage when exposed to the public internet.
- **Secure Defaults**: Shipping routers with secure configurations by default, such as strong, unique passwords, and disabled unnecessary services while users should be warned against insecure configurations.
- **Access Controls**: Restricting access to the router's web management interface from the LAN side by default and providing options to securely enable remote management if needed.
- **Encryption**: Utilizing strong encryption for the web management interface to protect communications between the router and the user.
- **Authentication**: Implementing strong authentication mechanisms, including the option for MFA, to secure access to the router's management interface.
- **Vulnerability Disclosure and Patching**: Establishing a clear, responsible disclosure policy for vulnerabilities and providing timely patches. This includes participating in the CVE program to track and disclose vulnerabilities.
- **End-of-Life Support**: Clearly communicating the end-of-life (EOL) policy for products and providing support and updates throughout the product's lifecycle are critical. For devices that are no longer supported, manufacturers should offer guidance on secure disposal or replacement.

3) Challenges and Considerations

- **Balancing Security and Usability**: One of the challenges is maintaining user-friendliness. Security measures should not overly complicate the user experience.
- **Cost Implications**: Developing secure products can incur additional costs. However, the long-term benefits of reducing the risk of breaches and attacks justify these investments.
- **Continuous Evolution**: Security is not a one-time effort but requires ongoing attention to adapt to new threats and vulnerabilities.
- **Building Trust**: By prioritizing security, manufacturers can build trust with customers, differentiating their products in a competitive market.
- **Engaging with Customers**: Actively engaging with customers to understand their security concerns and providing clear, accessible information on how to secure their devices.
- **Global Supply Chain**: routers are often produced as part of a complex global supply chain. Ensuring security across this chain, from component manufacturers to final assembly, requires coordination and adherence to security best practices at every stage.
- **Industry Collaboration**: Working with industry peers, security organizations, and regulatory bodies to establish and adhere to security best practices.

V. Consequences

- **Widespread Vulnerabilities**: A significant number of vulnerabilities, some 226 in total, collectively pose a substantial security risk.
- **Outdated Components**: Core components such as the Linux kernel and additional services like VPN or multimedia software in these routers are often outdated, making them susceptible to known exploits.
- **Default Passwords and Unencrypted Connections**: Many routers come with easy-to-guess default passwords and use unencrypted connections, which can be easily exploited by attackers.
- **Compromised Devices and Data**: Once a router is compromised, all devices protected by its firewall become vulnerable, allowing attackers to monitor, redirect, block, or tamper with data.
- **Risk to Critical Infrastructure**: Compromised routers can be used to attack critical infrastructure, potentially disrupting essential services in communications, energy, transportation, and water sectors.
- **DoS and Traffic Interception**: Vulnerabilities in protocols can lead to denial-of-service attacks against host services and interception of both internal and external traffic.
- **Eavesdropping and attacks**: Attackers can eavesdrop on traffic and launch further network-based attacks, making it difficult for users to detect a breach due to minimal router user interfaces.
- **Potential for Large-Scale Exploitation**: The sheer number of vulnerable devices, estimated in the millions, indicates a significant potential for widespread exploitation by malicious actors.
- **Legal and Technical Challenges**: Identifying specific vulnerable devices is complex due to legal and technical issues, which complicates the process of mitigating these vulnerabilities.