TLP:CLEAR

Secure by Design Alert

Security Design Improvements for SOHO Device Manufacturers

Malicious Cyber Actors Exploiting Insecure SOHO Routers

Threat actors—particularly the People's Republic of China (PRC)-sponsored Volt Typhoon group—are compromising small office/home office (SOHO) routers by exploiting software defects that manufacturers must eliminate through secure software design and development. Specifically, Volt Typhoon actors are exploiting security defects in SOHO routers to use them as launching pads to further compromise U.S. critical infrastructure entities. CISA and the Federal Bureau of Investigation (FBI) are releasing this Alert based upon recent and ongoing threat activity to urge SOHO router manufacturers to build security into technology products from the beginning and encourage all customers of SOHO routers to demand better security by design.

While PRC-sponsored actors, including the Volt Typhoon group, have made headlines by exploiting SOHO router software defects, the guidance for manufacturers to implement secure software design and development that can eliminate these defects is not new.

Secure by Design Lessons to Learn

A core tenet of secure by design is that manufacturers create safe and secure default behavior in the products they provide to customers. "Secure by Design" means that manufacturers design and build their products in a way that reasonably protects against malicious cyber actors successfully exploiting product defects. Incorporating this risk mitigation at the outset—beginning in the design phase and continuing through the release and updates—reduces the burden of cybersecurity on customers and risk to the public.

SOHO routers are ubiquitous and inexpensive devices that connect millions of Americans and small businesses to the internet. However, due to widespread sale, and subsequent use, of insecure SOHO routers that lack basic security features, threat actors, including the PRC-sponsored Volt Typhoon group, are exploiting these devices at scale. Additionally, these actors are leveraging compromised SOHO routers to move to and further compromise U.S. critical infrastructure entities. The creation of products that lack appropriate security controls is unacceptable given the current threat environment. This case exemplifies how a lack of secure by design practices can lead to real-world harm both to customers and, in this case, our nation's critical infrastructure.

Manufacturers often design and build SOHO routers that **lack automatic update capabilities** and include **high numbers of exploitable defects in web management interfaces,** which makes these devices vulnerable to common forms of compromise. Manufacturers compound these security issues by creating devices with management interfaces exposed to the public internet by default—often without notifying the customers of this frequently unsafe configuration.

Manufacturers should design, develop, and deliver SOHO routers with security and safety in mind to create product resiliency against foreseeable threats. CISA and the FBI encourage manufacturers to learn from the recent Volt Typhoon compromises by reviewing the principles set forth in Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. Additionally, manufacturers should review and follow the National Institute of Standards and Technology's Interagency Report (NIST IR) 8425 Internet of Things (IoT) Core Baseline and NIST's Preliminary Draft IoT Cybersecurity Profile for Consumer Grade Routers.

Principle 1: Take Ownership of Customer Security Outcomes

Principle 1 focuses on key security areas manufacturers should invest in to protect their customers as well as the public. These areas include setting default configurations that secure the devices against foreseeable threats. For example, SOHO router manufacturers should consider:

- Implementing automated and signed software updates to address security vulnerabilities, ideally without any user intervention. (See NIST IR 8425 "Software Update.")
- Placing the web management interface on LAN side ports to protect against vulnerable exposure.
- Improving the security of the management interface system to allow safe usage when exposed to the public internet, including by working to eliminate entire classes of vulnerability from the product.
- Setting secure defaults that customers must manually override and including sufficiently strong wording to dissuade them from doing so unless they have implemented compensating controls. (See NIST IR 8425 "Product Configuration.")

Principle 2: Embrace Radical Transparency and Accountability

Manufacturers should lead with transparency when disclosing product vulnerabilities. To that end, manufacturers should track the classes of vulnerability associated with their SOHO routers and disclose them to their customers via the CVE program. Manufacturers should ensure that their CVE records are correct and complete. It is especially important that manufacturers supply an accurate CWE so the industry can track classes of software defect, not just individual CVEs, and customers can understand areas where a given vendor's development practices may require improvement.[i] They should also identify and document the root causes of those vulnerabilities and declare it a business goal to work toward eliminating entire classes of vulnerability.

Principle 3: Build Organizational Structure and Leadership to Achieve These Goals

Just as software and hardware manufacturing executives care about cost, they should prioritize the security of their products. Leaders must consider the full picture: that customers, our economy, and our national security are currently bearing the brunt of business decisions to not build security into their products. Moreover, directing the business toward secure by design software development may reduce financial and productivity costs as well as complexity. Leaders should make the appropriate investments and develop the right incentive structures that promote security as a stated business goal.

Action Item for Software Manufacturers

Although this Secure by Design Alert focuses on how SOHO manufacturers can provide secure devices, it is just one part of a more comprehensive set of secure by design practices. To protect their customers from a wide range of malicious cyber activity, manufacturers should fully implement the principles and practices touched upon in this Alert by reviewing Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. Further, CISA urges manufacturers to publish their own secure by design roadmap to demonstrate that they are not simply implementing tactical controls but are strategically rethinking their responsibility in keeping customers safe.

[i] Common Weakness Enumeration (CWE) classification identifies classes of software/hardware weaknesses (including vulnerabilities and defects); Common Vulnerabilities and Exposures (CVE) classification identifies and labels unique vulnerabilities in specific software/hardware products.