eclypsium

BELOW THE SURFACE

THREAT REPORT

SUMMER 2024

ATTACKS VPN APPLIANCES • SECURING THE DIGITAL SUPPLY CHAIN

THE EVOLVING IoT THREAT • NEAT HARDWARE HACKING

INTRODUCTION

Welcome to the Below the Surface Threat Report. As the cybersecurity landscape continues to evolve, it's crucial to stay informed and proactive in defending against emerging threats. We hope this report provides you with valuable insights and strategies to enhance your organization's security posture. We highlighted some of the recent trends in the threat landscape in this edition, including attacks against VPN and firewall appliances and the ever-increasing attacks against IoT devices. Several new pieces of research were published, including new attacks against Windows drivers, hardware-based exploitation techniques, and supply chain attacks.

If you're not already subscribed to Below the Surface, you can do so at Eclypsium.com.

TABLE OF CONTENTS_

THREAT LANDSCAPE

Attacks Against VPN Appliances Continue

In recent months, there has been a surge in sophisticated attacks targeting VPN and firewall appliances from several major vendors. These attacks have leveraged critical severity-level vulnerabilities that cybercriminals exploit to gain access to an organization's networks. Notable incidents include:

- **Ivanti Connect Secure (Pulse Secure) VPN** - Attackers leveraged zero-day vulnerabilities to gain persistent access, allowing them to bypass authentication and establish backdoors for future intrusions.
- **Palo Alto PAN-OS** - Attackers began exploiting a 0-Day vulnerability in PAN-OS, eventually being tracked as CVE-2024-3400 with patches being released by Palo Alto. Attackers used several methods to gain persistent access to victim devices. Eclypsium now has detections for both the vulnerability and the observed malicious behaviors.
- **Zyxel USG Vulnerabilities** - While the vulnerabilities discovered by our research team are not present in the most recent version of Zyxel firmware (5.37), not everyone is always up-to-date. Zyxel has disabled the vulnerable ZTP service altogether as of V5.37 patch 1. Eclypsium notified Zyxel of the vulnerabilities but they declined to issue an advisory as the vulnerabilities are not present in the latest version of the firmware. However, since CVEs have not been issued for these vulnerabilities, organizations may not know that they need to update the firmware on their devices.
- **ArcaneDoor** - In April, Cisco's Talos research group published information on an espionage campaign targeting Cisco ASA firewall devices. The campaign utilized two zero-day vulnerabilities and had been active since November 2023. Two new implants were also discovered as part of the ArcaneDoor campaign that allowed attackers to remotely control devices and maintain persistence.
- **Velvet Ant** - A large organization suffered a major breach and attackers used a legacy F5 BIG-IP appliance as an internal C&C (Command and Control) server. The appliance (F5's BIG-IP product) is described as "The perfect place to hide" as they are deployed to trusted places in the network, exposed to the Internet, and visibility into operating-system level events is poor, or non-existent. An update to the Velvet Ant campaign described a new attack vector used by the threat actors: exploiting CVE-2024-20399 to elevate privileges. Attackers gained access to a Cisco NX-OS device, then used what was then a 0-Day exploit to break out of the Cisco networking interface and gain access to the Linux subsystem.

These incidents, and several others, highlight the critical need for supply chain security solutions and continuous monitoring of VPN and firewall appliances to protect against threat actors who are looking to evade detection and maintain persistence.

info@eclypsium.com
eclypsium.com

THREAT LANDSCAPE

Importance of Securing the Digital Supply Chain

Given recent attacks observed in the wild, securing the digital supply chain has never been more crucial. Attackers are increasingly targeting the supply chain to infiltrate organizations by exploiting vulnerabilities in third-party components and services. The supply chain attack against the open-source xz project was a clear reminder of the potential risk and underscored the importance of trust in the development lifecycle. A compromised supply chain can lead to widespread and devastating impacts, as seen in the SolarWinds attack, where malicious code was injected into the company's software updates, affecting numerous organizations globally.

A great example of the fragile supply chain was the incident where HP ProBooks were bricked due to alleged conflicts with Microsoft's Windows updates. Our technology infrastructure consists of many components and requires seamless integration across software (OS and applications), firmware, and hardware. As we enhance our supply chain risk mitigation strategies, OEMs and software vendors must prioritize transparency and integrity throughout the update and release process. This includes providing a comprehensive SBOM and maintaining SDLC artifacts.

Firmware updates are inherently complex, often involving multiple components within a single update package. For instance, a single UEFI or Intel ME update might include other components, or perform partial firmware updates through mechanisms like Capsule Updates. These processes typically require system reboots and are governed by hundreds of other critical parameters.

To mitigate these risks, organizations must:

- **Vet Suppliers Using The Eclypsium Guide** - Conduct thorough security evaluations of all third-party vendors and service providers to ensure they adhere to stringent security practices.
- **Implement Strong Controls** - Establish security controls and policies for managing and monitoring third-party components including hardware, firmware, and software. OEMs and software vendors should provide detailed SBOMs and SDLC artifacts to enhance supply chain security.
- **Continuously Monitor Assets in Production** - Employ continuous monitoring and threat intelligence to detect and respond to supply chain threats promptly. Implementing thorough pre- and post-update system state checks ensures compatibility and prevents conflicts.
- **Keep Firmware Up-to-Date and Validate Results** - A holistic approach to managing updates, including firmware, across all system components is crucial for maintaining security and functionality. To ensure a successful firmware update, it is essential to thoroughly assess the state of the system—including OS, firmware, and hardware—both before and after the update. This verification must be an integral part of the staging update process to prevent compatibility, and integration issues and maintain system integrity at scale.

RESOURCES

Infographic: A History Of Network Device Threats And What Lies Ahead

20,000 Fortinet devices breached by Chinese hackers – reboots, firmware updates no defence

Check Point Warning: VPN Gateway Products' Zero-Day Attack

Ivanti EPM SQL Injection Flaw Let Attackers Execute Remote Code

THREAT LANDSCAPE

The Evolving IoT Threat

Attacks targeting IoT devices, according to several different sources and reports, are at an all-time high. Many people dismiss the IoT threat and believe attacks are only targeting consumer devices (typically dubbed as a "router" that represents the device acting as a router, firewall, and Wi-Fi access point on a home network). However, several different classes of IoT devices exist in corporate and government networks, including IP cameras, NAS (Network Attached Storage), building automation, access control systems, printers, and VoIP (Voice over IP) devices—just to name a few types of devices. A trend being observed in today's threat landscape includes attackers discovering vulnerabilities and developing exploits for products that are end-of-life. In these cases the vendor no longer offers support, so vulnerabilities go unpatched allowing attackers to conduct campaigns where they can compromise devices at scale.

For example, several D-Link vulnerabilities were disclosed this year and added to the CISA KEV list, including:

- From CSRF to Unauthorized Remote Admin Access
- Sensitive information disclosure vulnerability in D-Link dir-605
- Command Injection and Backdoor Account in D-Link NAS Devices
- D-Link router DSL-2750B firmware 1.01 to 1.03 - remote command execution no auth required

A recent report from Forescout titled The Riskiest Connected Devices in 2024 calls out this growing problem:

"In 2024, attackers are crossing siloes to find entry points across the full spectrum of devices, operating systems and embedded firmware. Today, network equipment has become the riskiest IT device category surpassing endpoints. Threat actors are finding new vulnerabilities in routers and wireless access points — and are exploiting them quickly in massive campaigns. Similarly, IoT devices with vulnerabilities expanded a whopping 136% from a year ago."

RESOURCES

IoT Vulnerabilities Skyrocket, Becoming Key Entry Point for Attackers

Exploiting Routers to Make Them Safe - The lack of vendor-supplied patches has triggered some to create their own, creative, solutions. This project leverages a vulnerability and associated exploit to patch a vulnerability in a product no longer supported by the vendor.

Hacking Millions of Modems (and Investigating Who Hacked My Modem)

The Pumpkin Eclipse - Attackers caused a widespread outage affecting 600,000+ ISP customers by causing residential routers to enter a failure mode.

RESEARCH AND VULNERABILITIES

Neat Hardware Hacking

Security research helps us to understand how to defend our systems more effectively and the hardware security research listed below uncovers some important insights.

- **Mindshare: Decapping Chips For Electromagnetic Fault Injection (EMFI)** - While de-capping chips is not a new approach, this article describes a technique that allows for more accurate fault injection attacks. Caution: Do not try this at home as it uses dangerous chemicals!
- **TPM GPIO fail: How bad OEM firmware ruins TPM security** - Interesting attack against TPMs, described as: "In this article I demonstrate a software attack that allows an operating system to set the PCRs of a discrete TPM device to arbitrary values and unseal any secret that uses a PCR based sealing policy (such as disk encryption keys used by unattended unlock TPM FDE schemes)."

Google Pixel Updates

Pixel Update Bulletin—June 2024 - Before starting the vulnerability hunting and reverse engineering process for any new target it's highly beneficial to review security advisories, such as this one for Pixel Phones: https://lnkd.in/gvRjR5VQ These advisories reveal the multitude of components within a single phone, each with a complex architecture and running its own firmware. Each component contributes to the attack surface and contains known CVEs. For example, just in this advisory, there are 14 components—ACPM, CPIF, Exynos, Fingerprint, Goodix, GsmSs, LDFW, Mali, Modem, Pixel, Trusty, WLAN, SPI, and HWBCC—collectively associated with 32 CVEs, many of which are critical or high severity.

Windows Driver Vulnerabilities

As shown in the two articles listed below, attackers can abuse vulnerable Windows drivers to disable security tools such as EDR and deploy malware. To mitigate these threats, it is important to implement robust driver management policies, regularly audit and update installed drivers, and use Microsoft's recommended driver block rules.

- GhostEngine mining attacks kill EDR security using vulnerable drivers
- Vulnerable Driver segwindrvx64.sys in Insyde Software Corp SEG Windows Driver v100.00.07.02

Norway's NCSC Recommends Getting Rid Of Your VPN

Because VPN appliances have repeatedly shown themselves to be weak to attack, the Norwegian National Cyber Security Centre (NCSC) recommends that organizations begin replacing them with IPsec and IKEv2 solutions. They offer a goal of migrating to more secure solutions by 2025 and recommend limiting access and increased scrutiny of appliance logs as interim security mitigations.

HIGHLIGHTS

Cross-Execute Your Linux Binaries, Don't Cross-Compile Them

Enumerating System Management Interrupts

AutomationDirect P3-550E Telnet Diagnostic Interface leftover debug code vulnerability - Very interesting vulnerability and associated exploitation techniques.

Thecus NAS Firmware Decryption

CVE-2024-20356: Jailbreaking a Cisco appliance to run DOOM (Just for fun!)

ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices

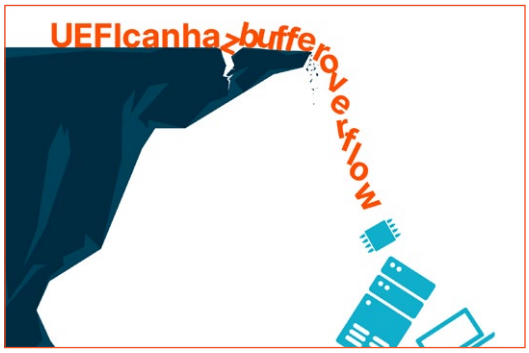
Dumping and extracting the SpaceX Starlink User Terminal firmware

RESOURCES

Further Reading

Recent Blog Posts

- Eclypsium Toolbox: Extending Supply Chain Security To New IT/ OT/IoT Devices
- UEFIcanhazbufferoverflow: Widespread Impact from Vulnerability in Popular PC and Server Firmware
- EPA Steps Up Cybersecurity Audits for Water Systems
- Bus Pirate 5: The Swiss ARRRmy Knife of Hardware Hacking
- Automata in Action: New Vulnerabilities Discovered in HP UEFI
- Windows Supply Chain Validation Cheat Sheet
- Big Vulnerabilities in Next-Gen BIG-IP



Recent Podcasts

- BTS #33 - Securing OT Environments - Dr. Ed Harris
- BTS #32 - Mitre ATT&CK - Adam Pennington
- BTS #31 - Managing Complex Digital Supply Chains - Cassie Crossley
- BTS #30 - Systems Of Trust – Robert Martin
- BTS #29 - Supply Chains, Firmware, And Patching - Jason Kikta

Recent Webinars

- Using Open Source and Built-In Tools for Supply Chain Validation
- Eclypsium Supply Chain Security Overview
- Eclypsium Automata - An Expert Researcher Never Sleeps

info@eclypsium.com
eclypsium.com