eclypsium®

Risk Management and Integrity Assurance for Network Devices

Network devices are critical to the health and security of any enterprise. Virtually every critical business or operational function directly depends on the switches, routers, VPNs, concentrators, gateways, firewalls, application delivery controllers, and other network devices at the heart of an organization.

However, these vital IT and security assets are often out of sight, out of mind when it comes to their own security. They're typically not covered by the standard security tools that organizations use to protect more common assets such as laptops and servers. Unfortunately, the combination of high strategic value and inconsistent protection has made network devices one of the most heavily targeted enterprise assets both by state-based threat actors as well as widespread ransomware campaigns. The same devices that historically have protected the enterprise are themselves under attack.

NETWORK DEVICES ARE UNDER SIEGE

Cyber threats are always evolving, and the shift to attacks against network devices has been one of the most significant developments in the past several years. In early 2020, CISA issued an alert that vulnerabilities in Citrix and Pulse Secure VPNs had become top targets for state-based threat actors. This would prove to only be the start of a larger trend as various state and ransomware-based attackers exploited an array of enterprise network devices and vendors.

OVERVIEW

WHO SHOULD READ THIS:

Security leaders, security practitioners, vulnerability management teams who need to protect their organization from recent attacks against network devices.

WHAT THEY WILL LEARN:

How network devices are being used in cyberattacks today, why traditional security tools often fail to protect them, and what new capabilities are required.

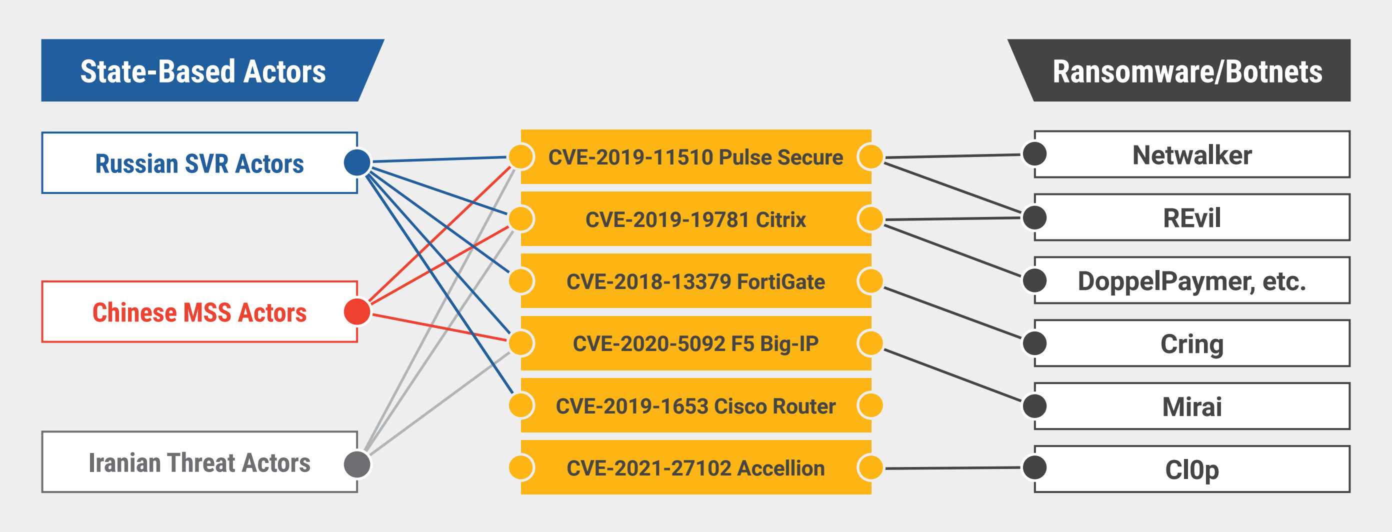
FURTHER READING:

- Assessing Enterprise Firmware Security Risk in 2021
- Applying Lessons From CISA to Your Firmware

Multiple alerts were issued detailing how Russian, Chinese, and Iranian state-based threat actors were targeting a variety of enterprise network devices and vendors. Notably, in one of the most recent alerts covering Russian SVR techniques, five of the top eleven targeted vulnerabilities (PDF) affected network devices.

But this isn't only a tactic of nation-state adversaries. Financially motivated attackers have adopted the same techniques for ransomware and malware campaigns. Netwalker was one of the first ransomware families to target network devices, and the trend quickly spread to some of the most popular ransomware groups including DoppelPaymer, Maze, and Ragnarok. The trend has only continued to accelerate with Cring ransomware targeting F5 devices in attacks against manufacturing plants. Most notably, REvil ransomware (aka Sodinokibi) is the most common ransomware in 2021 and has aggressively targeted F5 devices as well as PulseSecure VPNs. Most recently the highly targeted Cl0p ransomware exploited 0-day vulnerabilities in Accellion devices.

Compromised network devices can play a devastating role in all phases of a cyberattack, allowing attackers to manipulate or damage the central nervous system of the enterprise. Their publicly accessible nature can provide initial access into an organization. Their trusted position can then be used to spread malware through the organization or allow attackers to monitor, copy, or redirect traffic. Compromising network infrastructure can break the boundaries between IT/OT and other high value assets to cause damage, or attackers can directly "brick" network devices in order to cripple enterprise operations.



SECURITY ADVISORIES

U.S. AGENCIES SOUND THE ALARM ON NETWORK DEVICES

- **Joint NCSC-CISA-FBI-NSA Cybersecurity Advisory** (May 21, 2021) - Highlighted top exploits used by Russian SVR including 5 CVEs affecting network devices.
- **CISA Alert AA21-110A** (April 20, 2021) - Alert to a 0-day Pulse Secure vulnerability being exploited in the wild.
- **CISA Alert AA20-258A** (September 14, 2020) - Details Chinese MSS-affiliated actors targeting network devices.
- **CISA Alert AA20-259A** (September 15, 2020) - Details Iranian threat actors targeting network devices.
- **FBI Flash Alert MI-000130-MW** (July 28, 2020) - Alert to the increase of Netwalker ransomware attacks on US organizations and agencies targeting network devices.
- **CISA Alert AA20-073A** (March 13, 2020) - Highlights the need to keep VPN code up to date as workers increasingly work remotely.
- **CISA Alert AA20-133A** (May 12, 2020) - Noted a spike in attacks on Citrix and Pulse Secure network devices.

NETWORK DEVICES CREATE A CRITICAL SECURITY GAP

Network devices are a key part of an organization's security infrastructure. Ironically, security for these devices is often a blind spot in terms of cybersecurity. The traditional enterprise security controls that protect laptops and servers often can't be applied to network devices or lack the required visibility and specialization needed to address the types of threats seen in the wild. Several key challenges include:

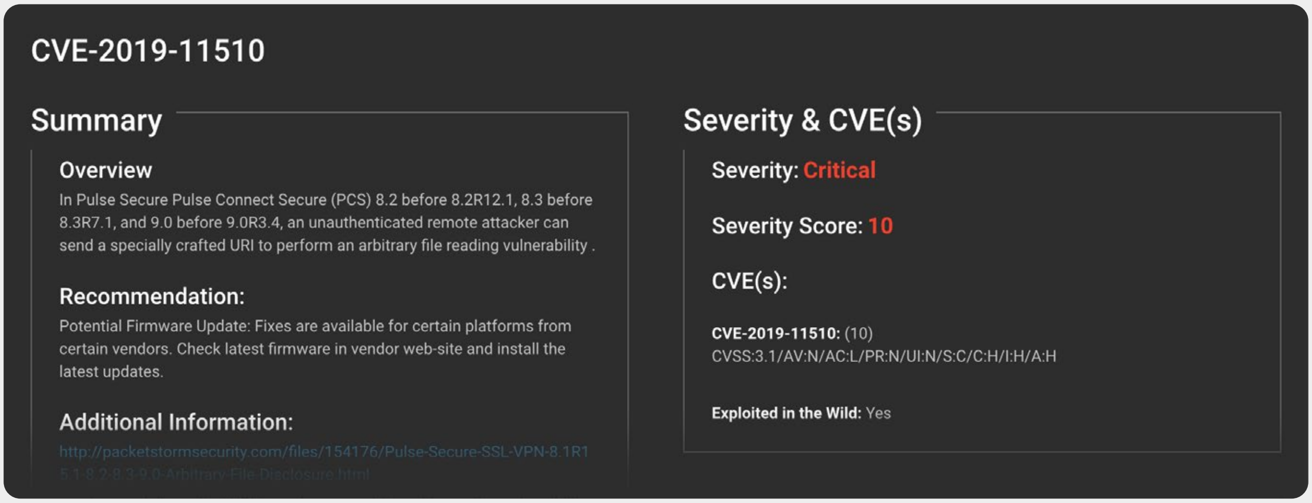
- **Lack of Support for Security Agents**
  Network devices typically don't support the traditional security agents that are applied to laptops and servers. While this is a common problem for IoT devices, network devices have much higher value and carry higher risk.
- **Proprietary OS Vulnerabilities**
  Network device vendors typically rely on their own custom-designed operating systems with their own unique vulnerabilities. However, these custom OSes typically don't receive the same industry-wide scrutiny or update processes found in standard operating systems, causing critical vulnerabilities to go unnoticed.
- **Out of Sight For Traditional Vulnerability Scanners**
  Traditional vulnerability scanners often fail to detect vulnerabilities in network devices, especially for vulnerabilities that reside within the firmware of the device. Even when traditional scanners support network device CVEs, it can be challenging for security teams to manage all the necessary plugins and to recognize the importance of network device vulnerabilities.
- **Lack of Threat Detection**
  Organizations have almost no way to identify devices that have been compromised as part of an attack. Any available tools are often one-off vendor-supplied tools offered in response to a specific threat. Most security teams simply don't have a way to verify the integrity of their network devices in a consistent way. The recent discovery of 0-day exploits in the wild highlights the need to detect compromises even from previously unknown threats.

DISCOVERY

DEVICE DISCOVERY THAT EMPOWERS SECURITY

Before security teams can protect their network devices, they naturally need to have visibility into what devices they have and where they are. However, this is often easier said than done in modern enterprise networks. Organizations may be highly distributed, with many routers, switches, VPNs, and firewalls, possibly from multiple vendors. Teams may lack central visibility into all these assets, or at best, visibility may be spread across multiple tools or owned by other teams.

Eclypsium's automated discovery of network devices ensures that security teams always have the independent visibility they need to support security operations. Eclypsium-managed endpoints automatically analyze their local environment to detect and classify network and other connected devices. This approach leverages the Eclypsium technology that is already deployed in the network without the need for network taps or complex network management tools. This ensures security teams always have a simple, up-to-date visibility of their network devices and attack surface.



CVE-2019-11510

Summary

Overview

In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability .

Recommendation:

Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:

http://packetstormsecurity.com/files/154176/Pulse-Secure-SSL-VPN-8.1R15.1-8.2-8.3-9.0-Arbitrary-File-Disclosure.html

Severity & CVE(s)

Severity: Critical

Severity Score: 10

CVE(s):

CVE-2019-11510: (10)
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Exploited in the Wild: Yes

ENSURING THE INTEGRITY OF NETWORK DEVICES

Eclypsium provides simple, automated security to the most critical layers of the most critical devices. Unlike traditional security which stops at the OS or application layers, Eclypsium extends security to the low-level code, firmware, hardware settings, and configurations that the higher software layers rely on. Security at this level is fundamental for network devices which rely on tightly integrated software, firmware, and hardware.

With Eclypsium, security teams can proactively discover their devices, then detect and respond to vulnerabilities, risks, and threats, all without having to deploy agents on the network devices themselves. Key capabilities include:

- **Automated Discovery and Visibility**
  The solution uses Eclypsium-managed endpoints to automatically discover network devices in the enterprise environment, making it easy to get up and running quickly and hone in on the devices that matter the most without the need for complex network management tools. The discovery process can be tightly controlled to protect user privacy and ensure that non-corporate environments are not analyzed.

- **Vulnerability and Risk Management**
  Eclypsium analyzes network devices for vulnerabilities with a special focus on CVEs actively exploited in the wild. This surfaces important overlooked vulnerabilities without adding extraneous noise to the organization's existing patch management process.

- **Threat Detection and Integrity Monitoring**
  Eclypsium analyzes a variety of code and firmware to ensure devices are only running valid, vendor-approved code. The solution verifies that the "known good" code from vendors hasn't been modified and checks for the presence of known threats.

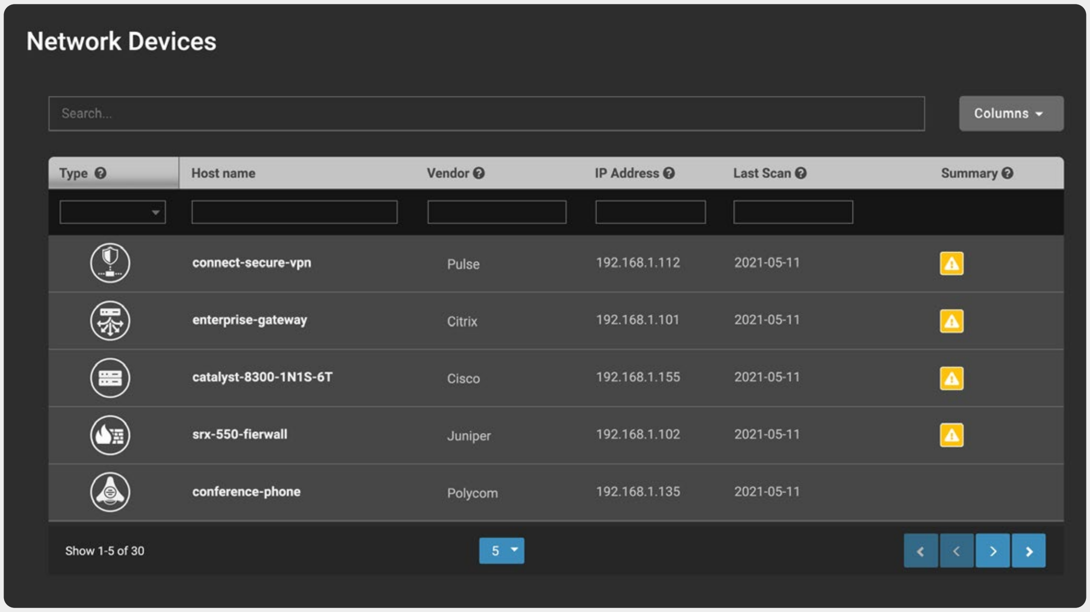
- **Multi-Vendor Support**
  Organizations may have multiple types of infrastructure, each with their own unique tools and processes. Eclypsium provides a single tool to support an ever-growing set of vendors including Cisco, Citrix, F5, Juniper, and Pulse Secure. This ensures teams can have a single, consolidated view of their device-level risk.

- **Agentless Security for Network Devices**
  Eclypsium's unique distributed approach means that security teams don't have to install a security agent on their network devices. This allows teams to easily get security visibility into devices without adding additional code or waiting on change windows.

- **Visibility Down to the Firmware**
  Many network device vulnerabilities, including those exploited in the wild, are tied to the firmware of the device. Eclypsium provides deeper visibility into these layers that are typically not seen by traditional scanners.

- **Converged Visibility and Risk Context**
  Eclypsium provides a unified view of the enterprise that includes laptops, servers, and network devices. This ensures that staff have a single place to see all their device-related risk without important context being locked in separate silos.

- **Remediation and Mitigation Support**
  The Eclypsium platform provides easy to use mitigation and remediation support for many firmware vulnerabilities or required updates. Rather than just telling you what's broken, Eclypsium helps you get back to full strength.



Network Devices

Type	Host name	Vendor	IP Address	Last Scan	Summary
	connect-secure-vpn	Pulse	192.168.1.112	2021-05-11	⚠
	enterprise-gateway	Citrix	192.168.1.101	2021-05-11	⚠
	catalyst-8300-1N1S-6T	Cisco	192.168.1.155	2021-05-11	⚠
	srx-550-fierwall	Juniper	192.168.1.102	2021-05-11	⚠
	conference-phone	Polycom	192.168.1.135	2021-05-11	

Show 1-5 of 30

Network devices continue to be one of the most active areas in cybersecurity. The landscape has evolved quickly over the past months and will likely continue to do so as attackers look for new vulnerabilities and advance their techniques. At Eclypsium we are dedicated to driving the industry forward with security research and controls to ensure that these critical devices remain as safe as possible. To learn more about the Eclypsium solution, please contact the team at info@eclypsium.com.

ABOUT ECLYPSIUM

Eclypsium is an enterprise device integrity platform for modern distributed organizations. The Eclypsium platform solves the latest and most potent device, firmware and supply chain integrity problems by identifying known and unknown devices throughout the enterprise, verifying current firmware and hardware against the world's largest database, and fortifying devices through automated configuration control and updates. Eclypsium was named a Gartner Cool Vendor in Security Operations and Threat Intelligence, a TAG Cyber Distinguished Vendor, one of the World's 10 Most Innovative Security Companies by Fast Company, a CNBC Upstart 100, a CB Insights Cyber Defender, and an RSAC Innovation Sandbox finalist. For more information, visit eclypsium.com.