EXTENDING VISIBILITY AND SECURITY TO NETWORK AND UNMANAGED DEVICES

Today we are excited to announce a major new extension to the Eclypsium device integrity platform, which lets organizations easily extend visibility and security beyond their traditional endpoints to all the network and unmanaged devices that can impact the security of their enterprise. Now available in beta, the new extension addresses traditional network gear like switches, routers, VPNs, application delivery controllers, and network-attached storage devices, as well as personal and unmanaged devices on the same network, helping enterprises to secure their ever-expanding attack surfaces.

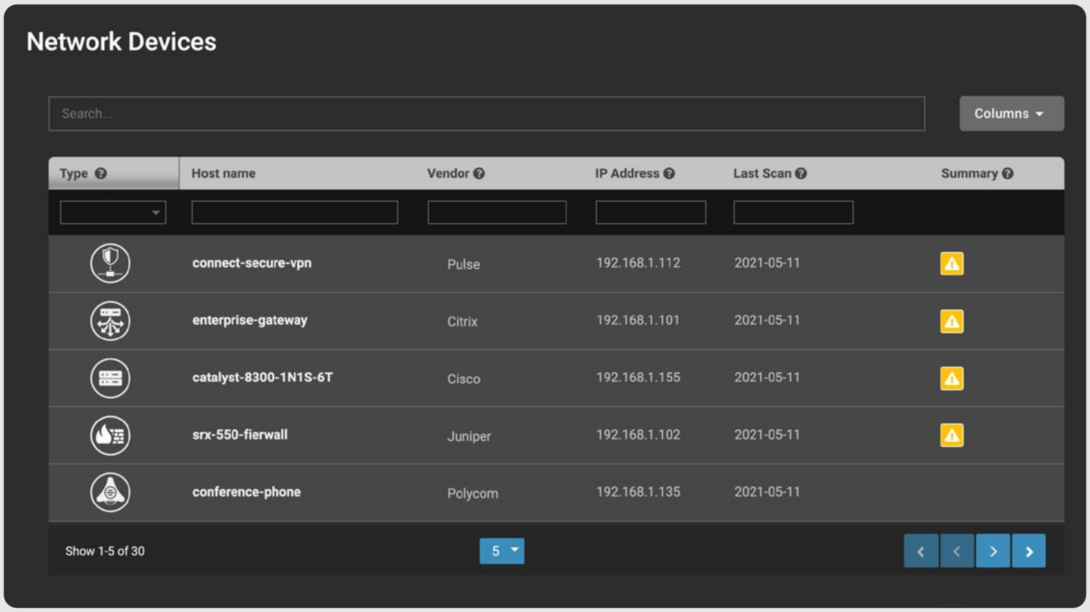
THE CHALLENGE

Modern organizations are in the midst of a transformation at the device level, and these changes are having profound impacts on their security. No longer defined simply by corporate laptops and servers, enterprises must navigate the risk of a constantly evolving landscape of networking equipment, connected devices, personal-use employee devices, as well as devices in their remote work environments. Many of these devices simply can't be managed using traditional security tools, with recent studies estimating that up to 90% of enterprise devices can't support a traditional security agent.

This unmanaged attack surface is actively under attack today. A recent Microsoft study found that 83% of businesses experienced a firmware attack in the past year. VPNs and networking infrastructure have been some of the most popular targets, as adversaries target them to gain access to organizations and spread ransomware and other malware. CISA has repeatedly issued alerts concerning a wide range of state-based actors targeting enterprise network infrastructure, including a recent May 7th joint advisory warning of active scanning and exploitation of leading vendors such as Cisco, Citrix, F5, Fortigate, Pulse Secure, and others.

> **"Network devices, like routers and switches, live and die by their firmware. In a world where firmware attacks and implants are on the rise, it's more critical than ever to ensure the integrity and security of these types of devices."**
>
> — Alek Amrani

The recent *Executive Order on Improving the Nation's Cybersecurity* makes it clear there's little distinction, in terms of the required level of assurance, between computing devices and network devices: "... software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources) — is a particular concern."



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

Unfortunately, most organizations aren't properly equipped to find these risks. Traditional scanning tools lack visibility into the all-important device and firmware layers, and many unmanaged devices are simply a persistent blind spot in an organization's security program.

NETWORK AND UNMANAGED DEVICES

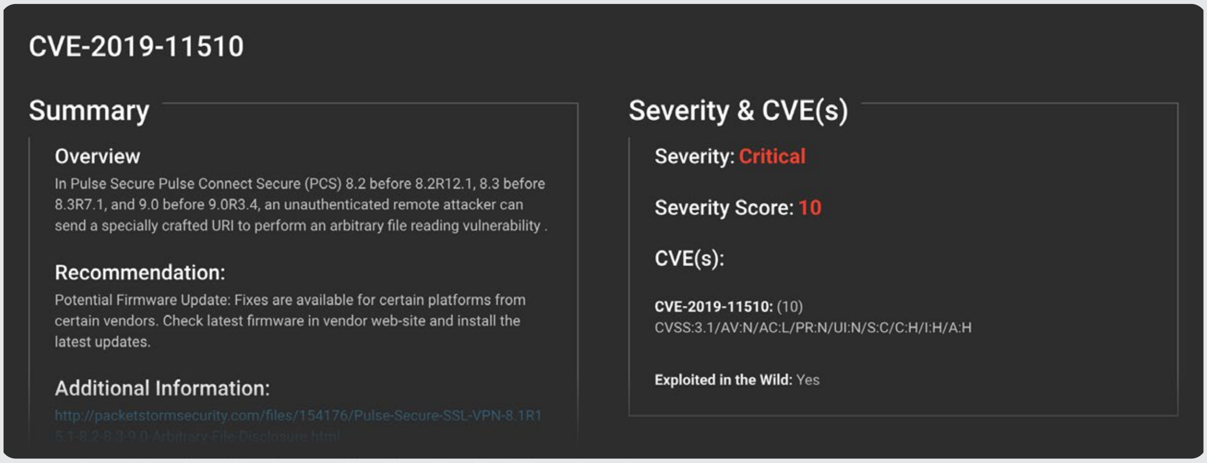
Eclypsium's new network device assessment capabilities, now in beta, provide organizations with an inventory and risk-based view of their network infrastructure, and other types of unmanaged devices, in addition to deep visibility on endpoints. Using its unique distributed approach to network device discovery and analysis, Eclypsium provides agentless visibility into all corners of an enterprise and can even identify risk to user devices when working remotely or during travel. Key capabilities include:

1. Distributed discovery of network and unmanaged devices by Eclypsium-managed endpoints removes the blind spots represented by connected but unchecked devices.
2. Automatic risk analysis of network infrastructure devices down to the firmware layer: switches, routers, and VPN gateways are assessed to identify critical vulnerabilities exploited in the wild.
3. Authenticated firmware integrity analysis of supported network devices assures that firmware has not been compromised.
4. Comprehensive dashboard of endpoints, servers, and unmanaged enterprise devices: see the entire estate and associated risks.
5. Automatically differentiate between corporate and external networks.
6. Converged view of overall risk: combine endpoint risk posture with the additional risk from connected devices, so security analysts understand the sum of combined endpoint + connected device risks.

With this expanded visibility and insight, organizations can achieve faster risk prioritization, rapidly mitigate threats, and discover known risks and potential threats across their entire IT infrastructure.

DEEP RISK ASSESSMENT FOR NETWORK DEVICES

Network devices such as VPNs, network controllers, and network gear such as switches and routers have become top targets for APT actors as well as ransomware operations. A recent joint alert from CISA and the FBI highlighted how attackers target network devices down to the firmware layer as a way to gain access to a network and move through target infrastructure. Unfortunately, recent 0-day attacks against Pulse Secure VPNs show that attackers continue to focus on network devices and uncover new vulnerabilities in this area.



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

Eclypsium's new capabilities help address this risk by providing deep automated analysis and vulnerability detection for enterprise network devices, including support for initial Cisco, Citrix, F5 Juniper, and Pulse Secure. The platform lets security teams see deeper into the device level where traditional vulnerability scanners lack visibility. Just as importantly, the solution leverages internal and industry threat intelligence to focus on the vulnerabilities that are actively under attack in the wild such as CVE-2019-11510, CVE-2019-19781, and CVE-2020-5902. This allows security teams to quickly focus on their immediate risk without adding noise to their vulnerability and patch management processes.

DISTRIBUTED DISCOVERY

Eclypsium brings a unique distributed approach to the discovery and monitoring of devices in the network, and optionally, in remote environments. The new capabilities give organizations the option to turn any host with a lightweight Eclypsium endpoint sensor into a distributed scanner to assess risk of all nearby network devices. The Eclypsium endpoint sensor can automatically detect whether the host is in a corporate or non-corporate external environment and then include or exclude discovery and assessment based on a predetermined policy.

This distributed approach to discover and assess network and unmanaged devices offers comprehensive and reliable visibility into all devices and the supply chain risk. Modern organizations are distributed and often have complex network structures, which now include remote and home offices. It is exceedingly difficult to establish visibility using traditional network scanning or network traffic analysis approaches. By using the perspective of managed endpoint devices with Eclypsium sensors, organizations can continuously discover and assess all network and unmanaged devices in proximity to these endpoints and maintain a comprehensive real-time inventory of all devices in their environment. It also gives organizations the ability to understand and manage the risk to remote user endpoints from all devices around, including when they are outside the confines of the corporate network.

CONVERGED VISIBILITY AND RISK CONTEXT

With our enhanced discovery and analysis capabilities, Eclypsium provides a single view of the enterprise that spans both managed and unmanaged devices. This ensures security and IT teams have a single place where they can see a true inventory of the devices in their environment. Next, Eclypsium can help teams understand the risks with those devices. This can include vulnerabilities or potential threats in a device or the risk posed by other devices in the vicinity.

Over the coming months, we will continue to add new discovery and risk analysis capabilities and expand support for new network devices. This will allow us to reliably discover all types of devices and continually enhance our visibility into vulnerabilities and threats across all enterprise devices. If you would like to learn more, please contact the Eclypsium team at info@eclypsium.com.