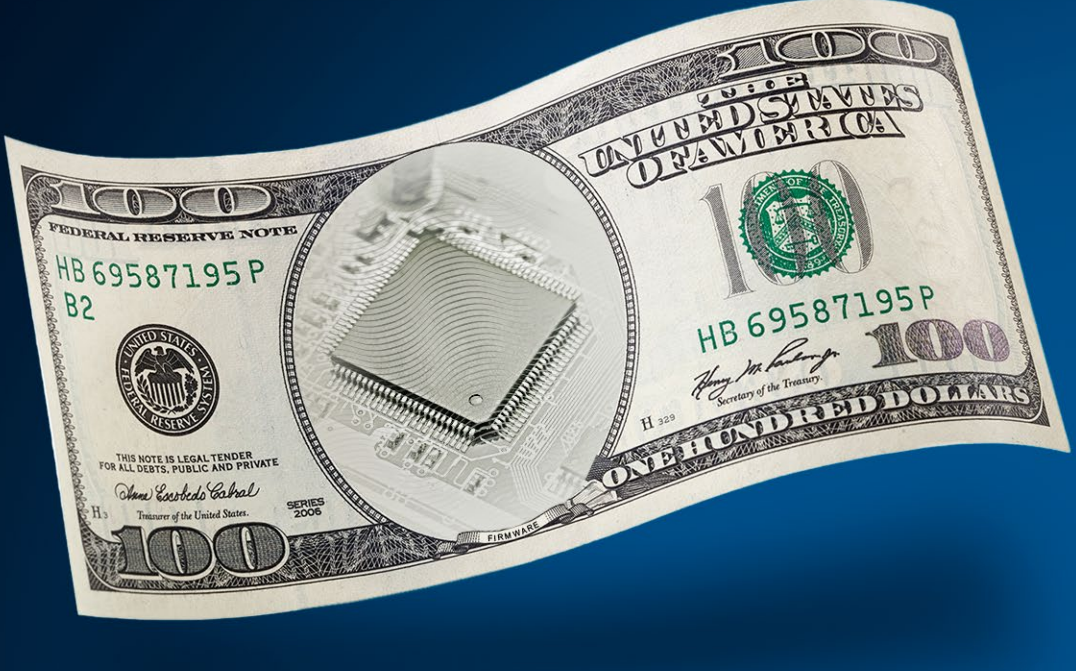


FIRMWARE: RANSOMWARE'S #1 ENABLER

Ransomware continues to be one of the most pervasive and damaging threats facing organizations today. While ransomware is not a new problem, attacks have recently seen massive growth in volume, sophistication, and most importantly, the damage caused to their victims. Enterprises are the most lucrative targets, and a mature and highly specialized ransomware economy has evolved dedicated to compromising enterprise infrastructure and avoiding enterprise security controls.

For many organizations, the firmware within their devices remains the least visible and least protected part of their attack surface. Ransomware actors have seized on this gap with a variety of new firmware-specific techniques, tools, and procedures (TTPs) that allow them to gain access and persist within an organization to cause the maximum amount of damage. Firmware within VPNs, networking devices, and security infrastructure have become some of the most common initial access vectors. Likewise, firmware threats within endpoint devices allows ransomware attackers to maintain persistence and subvert traditional OS-level controls.

This paper focuses on these and other recent developments in the ransomware landscape, and specifically the key role that firmware and device-level attacks play in attacks today. Readers will be able to learn:

- What's driving the latest growth and evolution of ransomware.
- How the ransomware economy works and what it means for enterprise firmware.
- How attackers use firmware in multiple phases of a ransomware attack.
- How ransomware is adopting techniques from the state-based threat actors.
- How to defend against ransomware at the firmware level.

As with all cybersecurity, ransomware defense requires a coordinated, layered approach. With this document security leaders and practitioners will be able to quickly learn the key role the firmware layer plays in real-world attacks and how firmware security can complement traditional security controls.

RANSOMWARE IS A GROWING PROBLEM

The enterprise risk of ransomware is at an all-time high as ransomware attacks continue to become more common, more damaging, and more expensive to organizations. A recent study found that ransomware attacks in North America have grown by 158% over the past years, driven by an increase in targeted attacks. The impact and pain caused to organizations also continue to rise with the average ransomware payment rising to more than $200,000 and average downtime increasing to 23 days.

The ongoing rise of ransomware is driven by a variety of factors. Notably, ransomware provides cybercriminals with a very direct path to making money. Instead of having to steal and resell data on black markets, ransomware actors can immediately monetize a successful attack by extorting the victim directly. This also means that many more types of enterprise data and systems are viable targets for attackers. In the past, could only focus on data that could be easily resold such as payment card data. In a ransomware attack, the data or systems that are disabled only have to be valuable to the victim. This means that virtually any data or systems that support an organization's operations are prime targets.

Recent developments such as the rise of double extortion schemes have only accelerated this trend. Ransomware that employs double extortion will exfiltrate sensitive data in addition, or in some cases instead of encrypting it. The attacker will then demand payment or threaten to make the information public. This naturally means that virtually any organizational secrets, intellectual property, or even private communications can be targeted by ransomware.

This creates a vastly expanded hunting ground for attackers. Virtually any organization can be targeted, and any sensitive data or system can be monetized.

RANSOMWARE ECONOMY

While it is common to refer to ransomware attacks or attackers, it is important to recognize that a ransomware event typically involves a variety of threat actors that are highly specialized in specific phases of an attack. This can include:

> **Ransomware Developers** - These developers build that actual ransomware itself. These developers specialize in malware to coordinate and encrypt data as quickly as possible in order to maximize damage to the enterprise. Developers will then sell their ransomware to other groups that will actually use the code in real-world attacks.
>
> **Initial Access Brokers (IABs)** - IABs are some of the most important pieces of the ransomware supply chain. These attackers specialize in gaining access to an enterprise and establishing a persistent presence that can then be resold to other criminals. This will often include some level of privilege escalation, lateral movement, and persistence techniques to ensure reliable access. As we will see, firmware exploits and techniques have become a critical part of the IAB arsenal.
>
> **Operators and Affiliates** - Ransomware operators and affiliates use the ransomware and access provided in previous phases to drive an actual ransomware attack. Some affiliates may specialize in additional lateral movement in order to maximize the impact of the attack. Operators will execute the actual ransomware and manage the extortion phase. Increasingly this phase can be delivered as a Ransomware-as-a-Service (RaaS) where an operator sells access to additional underlying affiliates.

This level of specialization allows attackers to cultivate more advanced techniques. Naturally, actors in each phase are highly prized for having techniques that are reliable and able to avoid and evade security controls.

THE ROLE OF FIRMWARE IN RANSOMWARE ATTACKS

Firmware has become a key component of ransomware attacks particularly in terms of gaining initial access and establishing ongoing persistence. Some ransomware groups have directly used firmware and boot-level attacks as a way to disable devices and lock their data. The "firmware-as-a-vector" preference for ransomware has become acute enough that Security Magazine called it out as one of the "6 common mistakes" practitioners make in an article on the persistence of ransomware from October 31, 2021.

Firmware and Network Devices for Initial Access

Firmware and device-level vulnerabilities within enterprise devices such as VPNs, application delivery controllers, and firewalls have become top entry points for ransomware groups. Ironically, vulnerabilities in the very devices trusted to protect the enterprise are now some of today's most active intrusion vectors.

This trend began in July of 2020, when the FBI issued an alert that Netwalker ransomware had begun targeting a Pulse Secure VPN vulnerability (CVE-2019-11510). This vulnerability was already being heavily exploited by multiple APT groups, and now ransomware was beginning to adopt the same techniques. Other ransomware groups quickly followed suit with REvil, Maze, and Black Kingdom all leveraging the same vulnerability.

The problem quickly spread to enterprise infrastructure vendors including Citrix, F5, Fortinet, Palo Alto Networks, and SonicWall. In very short order, dozens of ransomware groups including the top three of Maze, Conti, and REvil were all exploiting network devices for initial access. The table below highlights some of the more well-known ransomware groups that have been confirmed to attack network and infrastructure vulnerabilities in the wild.

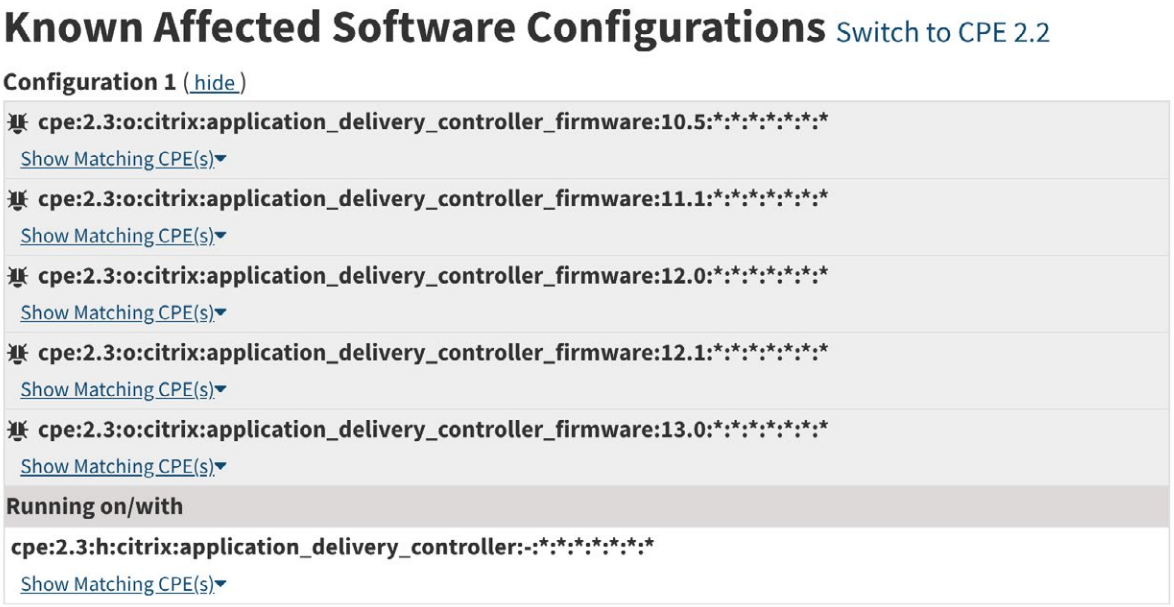
	Ransomware														
Vendor/Product	Agrius	BlackKingdom	Conti	Cl0p	Cring	Darkside	eChoraix	FIVEHANDS	Groove	Hello	Maze	Netwalker	Other	Pay2Key	REvil
Accellion				⚠											
Cisco				⚠											
Citrix									⚠		⚠		⚠		⚠
F5													⚠		
Fortinet	⚠		⚠		⚠									⚠	⚠
Microsoft Servers				⚠					⚠	⚠			⚠		
Oracle															⚠
Palo Alto Networks													⚠		
Pulse Secure		⚠							⚠		⚠	⚠	⚠		⚠
QNAP							⚠								
SonicWall						⚠		⚠		⚠					
Sophos													⚠		
VMware						⚠			⚠				⚠		

It is important to note that many of these vulnerabilities are directly tied to the firmware and integrated code of the network devices. For example, 12 of the 33 network device CVEs most commonly attacked by APTs and ransomware specifically name firmware as the affected component. This includes enterprise VPNs, Cisco routers, Citrix application delivery controllers, as well as SonicWall VPNs and security devices.

Even when firmware is not specifically named, much of the code within these infrastructure devices resides in integrated device code that will typically be missed by simple unauthenticated scans. Even if vulnerabilities are detected, they may not be appropriately prioritized by staff who tend to focus on more traditional operating systems and applications.

Problems get even worse when it comes to detecting threats or signs of compromise within enterprise infrastructure. Verifying the integrity of these devices will typically require manual, specialized tools, or one-off vendor-specific tools. This can make detections efforts slow and highly inconsistent.

PLATFORMS AFFECTED BY CITRIX VULNERABILITY CVE-2019-19781



Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:o:citrix:application_delivery_controller_firmware:10.5:*:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:o:citrix:application_delivery_controller_firmware:11.1:*:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:o:citrix:application_delivery_controller_firmware:12.0:*:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:o:citrix:application_delivery_controller_firmware:12.1:*:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:o:citrix:application_delivery_controller_firmware:13.0:*:*:*:*:*:*:*
Show Matching CPE(s)▾

Running on/with

cpe:2.3:h:citrix:application_delivery_controller:-:*:*:*:*:*:*:*
Show Matching CPE(s)▾

Source: https://nvd.nist.gov/vuln/detail/CVE-2019-19781

Firmware For Endpoint Persistence

After gaining initial access, IABs and ransomware affiliates are increasingly targeting firmware as a way to hide from security tools and persist within the environment. By implanting malicious code within firmware, attackers are able to subvert and persist below the operating system. Firmware implants and backdoors let attackers evade higher-level security controls, while also allowing malicious code to survive a complete reinstallation of the operating system. Such firmware implants have been seen in a variety of malware campaigns including MosaicRegressor and Lojax.

This strategy has been observed in TrickBot, which is the #1 most common form of malware affecting enterprises today. Trickbot is a highly modular trojan that specializes in lateral movement and persistence and is heavily used in Ryuk and Conti ransomware campaigns. TrickBot's new firmware capabilities known as TrickBoot, checks devices for well-known vulnerabilities that can allow attackers to read, write, or erase the UEFI/BIOS firmware of a device.

This functionality could have a devastating impact in the context of a ransomware attack. By writing malicious code into the firmware of a compromised device, the attacker could establish persistence within a device that would survive a complete re-imaging of the device. With control over the firmware of a device, an attacker would also be able to disable or evade security controls running the operating system. Or as a last resort, the attacker could simply corrupt the firmware in order to disable the device.

HOW TO DEFEND AGAINST RANSOMWARE AT THE FIRMWARE LEVEL

Firmware is both some of the most privileged and least protected code on enterprise devices today. As organizations have improved security at the operating system level, ransomware and other threat actors are increasingly being driven to the comparatively unguarded firmware layer.

To defend against ransomware, organizations must ensure that their firmware gets the same levels of visibility and protection as other critical code such as operating systems and applications. For most organizations this will require adding firmware-specific processes and tooling to support the following key phases of firmware security:

1. **Identify Firmware** - Establish full visibility over the firmware attack surface. Automatically discover all critical devices including network and security devices commonly exploited as initial ransomware vectors. Gain visibility of the firmware and device-level configurations used in all critical devices.

2. **Verify Firmware** - Proactively identify vulnerabilities in firmware, prioritizing those that are being used in real-world ransomware attacks. Actively check the integrity of all firmware and monitor firmware behavior to identify signs of threats or compromise.

3. **Fortify Firmware** - Update vulnerable firmware and ensure all available security features are enabled and properly configured.

The Connection Between APT and Ransomware Threat Actors

In cybersecurity, it is common to see financially motivated attackers mimic the tools and techniques first used by APT actors. The abuse of firmware by ransomware provides a case in point.

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 a series of additional alerts detailed 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. In fact, the vast majority of the network device vulnerabilities exploited by ransomware were previously used in nation-state attacks. This means that enterprises may want to keep track of the device vulnerabilities targeted by APTs as a leading indicator of where ransomware can be expected to go in the future.

Likewise, firmware implants were observed in APT and other nation-state backed operations long before they were seen in TrickBot. The 2015 disclosure of the Hacking Team's UEFI implant provided an example of how APT actors were already using firmware implants in their operations. This same code was later reused in MosaicRegressor, further highlighting how firmware capabilities can easily be incorporated by other threats

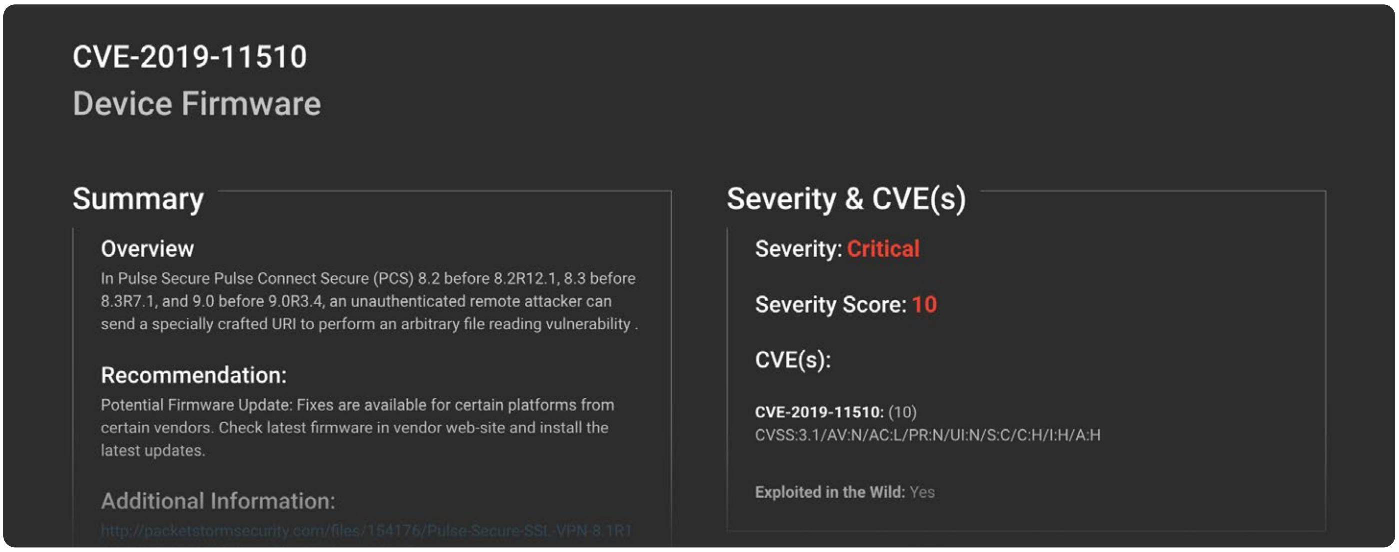
State-based threat actors have also employed ransomware directly in their operations. This was seen in some of the most well-known attacks such as the Russian involvement with the infamous NotPetya attacks. Similarly, DPRK threat actors have been linked to TrickBot, while Iranian actors have been tied to the Agrius family of ransomware.

As a result, organizations should recognize that there is not a just a single type of actor or motivation when it comes to ransomware. As with all threats, security teams must be prepared to defend against broad, opportunistic ransomware attacks as well as more targeted operations.

Eclypsium's firmware security platform provides a simple, automated way for organizations to address these needs consistently across all their critical device types and vendors. In the context of defending against ransomware, Eclypsium allows teams to take the following actions:

Discover Critical Devices - Eclypsium can automatically discover devices in the enterprise environment including network devices that are heavily targeted by ransomware actors. Eclypsium's unique distributed discovery allows teams to discover these critical devices without having 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.

Find Firmware Vulnerabilities and Risks - Eclypsium analyzes enterprise devices for vulnerabilities with a special focus on CVEs and other weaknesses that are actively exploited in the wild. This surfaces important overlooked vulnerabilities without adding extraneous noise to the organization's existing patch management process. Teams can quickly identify vulnerable network devices that are targeted by ransomware and easily find endpoints that are susceptible to TrickBot/TrickBoot. The solution also ensures that all available security features are enabled and properly configured.



CVE-2019-11510
Device Firmware

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-8.1R1

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

Patch and Update Vulnerable Devices - Eclypsium lets teams easily update firmware and device code to remediate vulnerabilities and trigger automated alerts and workflows to respond to security events. Staff can remediate problems directly through the Eclypsium console or via API to download and install firmware updates.

Verify Device Integrity and Detect Threats - 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. The platform also performs behavioral analysis where applicable in order to identify potential unknown threats. This can identify network devices or endpoints that may have been compromised by a IAB or ransomware operator.

These key capabilities arm security teams with the tools to protect their assets from ransomware at the firmware level. As with any active area of cybersecurity, attackers are constantly evolving and seeking out new vulnerabilities and techniques. Eclypsium specializes in the critical areas of firmware security and network devices, and our industry-leading research ensures organizations stay up to date even as new risks and threats emerge. To learn more about the Eclypsium platform, please contact us at info@eclypsium.com.