

# CVE-2020-1472: Advanced Persistent Threat Actors Use Zerologon Vulnerability In Exploit Chain with Unpatched Vulnerabilities

[tenable.com/blog/cve-2020-1472-advanced-persistent-threat-actors-use-zerologon-vulnerability-in-exploit-chain](https://tenable.com/blog/cve-2020-1472-advanced-persistent-threat-actors-use-zerologon-vulnerability-in-exploit-chain)

October 12, 2020



[Satnam Narang](#) | [Cyber Exposure Alerts](#)

October 12, 2020 | 7 Min Read

CYBER EXPOSURE ALERT

# VULNERABILITY EXPLOITED

U.S. Government agencies issue joint cybersecurity advisory cautioning that advanced threat groups are chaining vulnerabilities together to gain entry into government networks and elevate privileges.

**Update October 13, 2020:** The Identifying affected systems section has been updated to include details about the availability of a Zerologon scan template for Tenable.io, Tenable.sc and Nessus.

## Background

On October 9, the Cybersecurity Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) [published a joint cybersecurity advisory](#). The advisory, identified as Alert AA20-283A, provides insight into advanced persistent threat (APT) actors' activity against networks associated with federal and [state, local, tribal, and territorial](#) (SLTT) governments. The alert details how APT actors are using vulnerability chaining or exploit chaining, incorporating a recently disclosed elevation of privilege vulnerability in their attacks.

The following is a list of vulnerabilities referenced in the CISA/FBI joint cybersecurity alert:

CVE	Vendor/Product	CVSSv3	Tenable VPR*	Disclosed
<a href="#">CVE-2019-11510</a>	Pulse Connect Secure SSL VPN	10.0	10.0	Apr 2019
<a href="#">CVE-2018-13379</a>	Fortinet FortiOS SSL VPN	9.8	9.8	May 2019

<b>CVE</b>	<b>Vendor/Product</b>	<b>CVSSv3</b>	<b>Tenable VPR*</b>	<b>Disclosed</b>
<a href="#"><u>CVE-2019-19781</u></a>	Citrix Netscaler	9.8	9.9	Dec 2019
<a href="#"><u>CVE-2020-1631</u></a>	Juniper Junos OS	9.8	6.7	Apr 2020
<a href="#"><u>CVE-2020-2021</u></a>	Palo Alto Networks PAN-OS	10.0	10.0	Jun 2020
<a href="#"><u>CVE-2020-5902</u></a>	F5 BIG-IP	9.8	9.9	Jul 2020
<a href="#"><u>CVE-2020-15505</u></a>	MobileIron	9.8	9.5	Jul 2020
<a href="#"><u>CVE-2020-1472</u></a>	Microsoft Netlogon	10.0	10.0	Aug 2020

\*Please note Tenable VPR scores are calculated nightly. This blog post was published on October 12 and reflects VPR at that time.

## Analysis

### Initial access gained through SSL VPN vulnerability

According to the CISA/FBI alert, the APT actors are “predominantly” using CVE-2018-13379 to gain initial access to target environments.

CVE-2018-13379 is a path traversal vulnerability in Fortinet’s FortiOS Secure Socket Layer (SSL) virtual private network (VPN) solution. It was patched by Fortinet in April 2019. However, it wasn’t until after exploitation details were made public in August 2019 that [reports emerged of attackers exploiting it in the wild](#).

In addition to the Fortinet vulnerability being used to gain initial access, CISA/FBI have also observed “to a lesser extent,” APT actors using CVE-2020-15505, a remote code execution vulnerability in MobileIron’s Core and Connector.

### Post exploitation elevation of privilege using Zerologon

Once the APT actors have gained an initial foothold into their target environments, they are elevating privileges using CVE-2020-1472, a critical [elevation of privilege vulnerability in Microsoft’s Netlogon](#). Dubbed “Zerologon,” the vulnerability has gained notoriety after it was initially patched in [Microsoft’s August Patch Tuesday release](#).

On September 18, CISA [issued Emergency Directive 20-04](#) in an effort to ensure Federal Civilian Executive Branch systems were patched against the vulnerability.

### Zerologon observed as part of attacks in the wild

On September 23, Microsoft's Security Intelligence team tweeted that they had observed the Zerologon exploits being "incorporated into attacker playbooks" as part of threat actor activity.

Microsoft is actively tracking threat actor activity using exploits for the CVE-2020-1472 Netlogon EoP vulnerability, dubbed Zerologon. We have observed attacks where public exploits have been incorporated into attacker playbooks.

— Microsoft Security Intelligence (@MsftSecIntel) September 24, 2020

In a follow-up tweet on October 6, Microsoft's Security Intelligence team noted a new campaign leveraging CVE-2020-1472 originating from a threat actor known as CHIMBORAZO, also known as TA505, a financially motivated nation-state actor.

We're seeing more activity leveraging the CVE-2020-1472 exploit (ZeroLogon). A new campaign shrewdly poses as software updates that connect to known CHIMBORAZO (TA505) C2 infrastructure. The fake updates lead to UAC bypass and use of wscript.exe to run malicious scripts.

— Microsoft Security Intelligence (@MsftSecIntel) October 6, 2020

### **CISA/FBI warn of additional vulnerabilities being targeted for initial access**

In addition to the Fortinet and MobileIron vulnerabilities identified in recent campaigns, the CISA/FBI alert also warns that these APT threat actors may also leverage one of the following vulnerabilities to gain entry into their targeted networks:

- CVE-2019-11510 is an arbitrary file disclosure vulnerability in Pulse Connect Secure SSL VPN
- CVE-2019-19781 is a path traversal vulnerability in Citrix Application Delivery Controller (ADC), Citrix Gateway and Citrix SD-WAN WANOP appliances
- CVE-2020-1631 is a local file inclusion (LFI) vulnerability in Juniper's Junos OS HTTP/HTTPS service
- CVE-2020-2021 is an authentication bypass vulnerability in the Security Assertion Markup Language (SAML) authentication in PAN-OS when certain prerequisites are met
- CVE-2020-5902 is a path traversal vulnerability in the traffic management user interface (TMUI) in F5's BIG-IP application delivery service.

### **Evergreen vulnerabilities remain popular amongst threat actors**

Many of the vulnerabilities referenced in this joint alert from CISA/FBI have become evergreen flaws for threat actors. As part of CISA's Top 10 Routinely Exploited Vulnerabilities alert, they reference both the Pulse Secure and Citrix ADC vulnerabilities.

In September, CISA issued two separate alerts ([AA20-258A](#), [AA20-259A](#)) that highlight how APT actors from China and Iran are targeting unpatched vulnerabilities in Pulse Connect Secure, Citrix ADC, and F5's BIG-IP.

### **Elections support systems accessed, yet elections data integrity intact**

In Alert AA20-283A, CISA mentions that they observed activity that “resulted in unauthorized access to elections support systems.” However, they also mention that despite said unauthorized access, they have no evidence to support that the “integrity of elections data has been compromised.”

### **Zerologon needs to be patched immediately**

With the latest alert from CISA and the FBI, coupled with reporting from other vendors, it seems clear that Zerologon is becoming one of the most critical vulnerabilities of 2020.

### **Proof of concept**

---

A number of proofs-of-concept (PoC) and exploit scripts were made available soon after these vulnerabilities were publicly disclosed. The following is a subset of some of the PoCs and exploit scripts:

<b>CVE</b>	<b>Source URL</b>
CVE-2018-13379	<a href="#">GitHub</a>
CVE-2018-13379	<a href="#">GitHub</a>
CVE-2018-13379	<a href="#">GitHub</a>
CVE-2019-11510	<a href="#">GitHub</a>
CVE-2019-11510	<a href="#">GitHub</a>
CVE-2019-11510	<a href="#">GitHub</a>
CVE-2019-19781	<a href="#">GitHub</a>
CVE-2019-19781	<a href="#">GitHub</a>
CVE-2019-19781	<a href="#">GitHub</a>
CVE-2020-5902	<a href="#">GitHub</a>
CVE-2020-5902	<a href="#">GitHub</a>
CVE-2020-5902	<a href="#">GitHub</a>
CVE-2020-15505	<a href="#">GitHub</a>

<b>CVE</b>	<b>Source URL</b>
CVE-2020-1472	<a href="#">GitHub</a>
CVE-2020-1472	<a href="#">GitHub</a>
CVE-2020-1472	<a href="#">GitHub</a>

## Solution

Patches are available for all of the vulnerabilities referenced in the joint cybersecurity advisory from CISA and the FBI. Most of the vulnerabilities had patches available for them following their disclosure, with the exception of CVE-2019-19781, which received patches a month after it was originally disclosed.

Please refer to the individual advisories below for further details.

<b>CVE</b>	<b>Patch Information</b>
CVE-2019-11510	<a href="#">SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX</a>
CVE-2018-13379	<a href="#">FG-IR-18-384: FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests</a>
CVE-2019-19781	<a href="#">Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance</a>
CVE-2020-1631	<a href="#">2020-04 Out of Cycle Security Advisory: Junos OS: Security vulnerability in J-Web and web based (HTTP/HTTPS) services</a>
CVE-2020-2021	<a href="#">PAN-OS: Authentication Bypass in SAML Authentication</a>
CVE-2020-5902	<a href="#">K52145254: TMUI RCE vulnerability CVE-2020-5902</a>
CVE-2020-15505	<a href="#">July 2020: MobileIron Security Updates Available</a>
CVE-2020-1472	<a href="#">Netlogon Elevation of Privilege Vulnerability</a>









## Identifying affected systems

---

A list of Tenable plugins to identify these vulnerabilities can be found here:

Tenable.io, Tenable.sc and Nessus users can use a new scan template dedicated to targeting Zerologon. Plugin [140657](#) and its dependencies are automatically enabled within the template, and it also comes with the required settings automatically configured.

### Tactical Scans

 <b>Badlock Detection</b> Remote and local checks for CVE-2016-2118 and CVE-2016-0128.	 <b>Bash Shellshock Detection</b> Remote and local checks for CVE-2014-6271 and CVE-2014-7169.	 <b>DROWN Detection</b> Remote checks for CVE-2016-0800.
 <b>Malware Scan</b> Scan for malware on Windows and Unix systems.	 <b>Shadow Brokers Scan</b> Scan for vulnerabilities disclosed in the Shadow Brokers leaks.	 <b>Spectre and Meltdown Detection</b> Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754
		
 <b>Zerologon Remote Scan</b> A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).		

## Get more information

---

***Join [Tenable's Security Response Team](#) on the Tenable Community.***

***Learn more about [Tenable](#), the first Cyber Exposure platform for holistic management of your modern attack surface.***

Get a [free 30-day trial](#) of Tenable.io Vulnerability Management.



## **Satnam Narang**

---

Satnam joined Tenable in 2018. He has over 15 years experience in the industry (M86 Security and Symantec). He contributed to the Anti-Phishing Working Group, helped develop a Social Networking Guide for the National Cyber Security Alliance, uncovered a huge spam botnet on Twitter and was the first to report on spam bots on Tinder. He's appeared on NBC Nightly News, Entertainment Tonight, Bloomberg West, and the Why Oh Why podcast.

**Interests outside of work:** Satnam writes poetry and makes hip-hop music. He enjoys live music, spending time with his three nieces, football and basketball, Bollywood movies and music and Grogu (Baby Yoda).



## **Are You Vulnerable to the Latest Exploits?**

---

Enter your email to receive the latest cyber exposure alerts in your inbox.