secpod

TOP VULNERABILITIES REPORT 2020

www.secpod.com

secpod

INDEX

Time and again, software vulnerabilities have proved to be the most exploited attack vectors of security breaches and ransomware attacks. When threat actors target a particular network, their first move is to identify publicly disclosed vulnerabilities in an unpatched state. Hackers identify an unpatched vulnerability, execute the attack, and compromise the network to spread malware or steal data.

Vulnerabilities are the first and preferred target when hackers plan to execute a targeted attack. Hackers look for publicly disclosed and relatively old vulnerabilities in endpoints and exploit them. In fact, IDC has found that in 2019, **70 percent** of security breaches originated at an endpoint. From repeated past events like these, we can note that vulnerability management is one of the most important security measures for preventing cyber-attacks.

This report contains a list of endpoint vulnerabilities from January 2020 to December 2020 that have either caused severe damage or pose severe risks.

WHICH VULNERABILITIES ARE INCLUDED IN THIS REPORT?

Every year, thousands of vulnerabilities are disclosed publicly by security researchers worldwide. This report is a compilation of the top vulnerabilities found in software pertaining to desktops, laptops, and servers. They may be operating systems, network management applications, and other third-party applications installed in these devices which might have been exposed by the vulnerability.

A vulnerability gets included in this list based on two factors:

01 High and critical risk levels

The CVSS (common vulnerability scoring system) is designed to provide open and universally standard severity ratings of software vulnerabilities. A vulnerability with a CVSS v3 score of 7.0 to 8.9 is rated highly critical. A score of 9.0 to 10.0 is considered severely critical. All vulnerabilities included in this report are given a score of 8.0 or above with a few exceptions.

02 Exploit activity/potential

Vulnerabilities with lower severity ratings may not be actively exploited in the real-world. Although, when there are warnings about easy or active exploitation, we can infer that hackers will find it easy or advantageous to exploit the vulnerabilities. All vulnerabilities included in this report have either caused damage or pose serious risks to businesses and their reputation.

TOP VULNERABILITIES OF 2020

Based on the factors mentioned above, these 20 vulnerabilities are the ones posing maximum risk to a business. If you still have not remediated these vulnerabilities, we strongly recommend you do so because the possibility of an exploit is still high.

Please note that the list number preceding a vulnerability does not correspond to the impact caused by the vulnerability. All vulnerabilities carry roughly the same level of impact/risk.

01 CRITICAL VULNERABILITY IN OPENSMPTD

CVE	CVSS 3.0	Severity	Disclosed on	Affected product
CVE-2020-7247	9.8	Critical	January 29th, 2020	OpenBSD version 6.6

Details of the vulnerability

OpenSMTPD is a Unix daemon which implements the Simple Mail Transfer Protocol to deliver messages on a local machine or to relay them to other SMTP servers. The flaw was discovered in the code of a delivery agent which could allow the attacker to elevate privileges and run arbitrary code. It is known to be exploitable since May 2018. More details about the vulnerability **here.**

Impact

Successful exploitation allows attackers to run shell commands with root privileges.

Victims

There is no evidence about the exploitation of this vulnerability.

Solution

OpenBSD has released a patch to mitigate the vulnerability.

02 CRITICAL VULNERABILITIES IN GOOGLE CHROME

CVE	CVSS 3.0	Severity	Disclosed on	Affected product
CVE-2020-6407 CVE-2020-6418	8.8 6.5	Critical Medium	February 27th 2020	Google Chrome versions before 80.0.3987.122 Microsoft Chromium-based Edge versions before 80.0.361.62

Details of the vulnerability

A total of three vulnerabilities were disclosed, out of which two were zero-days and one was not allotted a CVE number. The vulnerability CVE-2020-6418, is a type confusion vulnerability and is associated with a side-effect in Chrome's V8 engine. It could lead to arbitrary remote code execution. The second vulnerability CVE-2020-6407 is associated with the streams API, which is used to break down and process a resource, bit by bit. The third vulnerability, which has not been assigned a CVE, arises due to an integer overflow in ICU. More details about the vulnerabilities **here.**

Impact

These vulnerabilities could allow a remote attacker to execute arbitrary code on the affected systems.

Victims

These vulnerabilities have been reported to be exploited in the wild.

Solution

Google has released a patch to mitigate these vulnerabilities.

03 CRITICAL VULNERABILITIES IN CISCO PRODUCTS

CVE	CVSS 3.0	Severity	Disclosed on
CVE-2020-3119	8.8	High	February 5th 2020
CVE-2020-3118	8.8	High	
CVE-2020-3111	8.8	High	
CVE-2020-3110	8.8	High	
CVE-2020-3120	6.5	Medium	

Affected products

Routers	Switches
ASR 9000 Series Aggregation Services Routers	Nexus 1000 Virtual Edge and Nexus 1000V Switch
Carrier Routing System (CRS)	Nexus 3000, 5500, 5600, 6000 and 7000 Series Switches
Firepower 1000, 2100 and 4100 Series	Nexus 9000 Series Fabric Switches
Firepower 9300 Security Appliances	MDS 9000 Series Multilayer Switches
IOS XRv 9000 Router	Network Convergence System (NCS) 1000, 5000, 540, 5500, 560 and 6000 Series
White box routers running Cisco IOS XR	UCS 6200, 6300 and 6400 Series Fabric Interconnects
IP Phones	**IP Cameras**
IP Conference Phone 7832 and 8832	Video Surveillance 8000 Series IP Cameras
IP Phone 6800, 7800, 8800 and 8851 Series	
Wireless IP Phone 8821 and 8821-EX	
Unified IP Conference Phone 8831	

Details of the vulnerability

Armis Security Inc. discovered all five vulnerabilities in CDP (Cisco Discovery Protocol), a proprietary Layer 2 protocol developed by Cisco Systems. The vulnerabilities were collectively termed CDPwn. Attackers can exploit these newly disclosed vulnerabilities to takeover vulnerable Cisco devices. An attacker can exfiltrate data of corporate network traffic traversing through an organization's switches and routers and view sensitive information such as phone calls from IP phones and video feeds from IP cameras. More about the vulnerabilities **here.**

Impact

Out of the five vulnerabilities disclosed by Cisco Systems, four are can lead to Remote Code Execution (RCE) while one (CVE-2020-3120) can cause Denial of Service (DoS) impacting an entire enterprise.

Victims

There is no evidence about the exploitation of these vulnerabilities. Although millions of enterprise devices are at serious risk.

Solution

Cisco has released patch updates to fix all these vulnerabilities.

04 GHOSTCAT VULNERABILITY IN APACHE TOMCAT SERVER

CVE	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-1938	9.8	Critical	February 24th 2020	Apache Tomcat version 6.x, 7.x before 7.0.100, 8.x before 8.5.51 and 9.x before 9.0.31

Details of the vulnerability

The vulnerability was more than a decade old when it was discovered. The flaw was discovered in Tomcat AJP protocol by researchers at Chaitin Tech. It allows attackers to read or include any files in the web application directories of Tomcat. The impact is known to be much severe in cases where the application allows the uploading of files. An attacker can upload a malicious file, and then include it using the Ghostcat vulnerability. This could result in the remote execution of malicious code.

Impact

An attacker can execute malicious code and also read sensitive information from the configuration files and source code files of all web applications which run on Tomcat.

Victims

There is no evidence about exploitation of this vulnerability although it has been around for a decade.

Solution

Apache has released fixes for this vulnerability in Tomcat. Refer to **this article** for the fixes.

05 VULNERABILITIES IN TREND MICRO SECURITY PRODUCTS

CVE	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-8467 CVE-2020-8468	8.8 8.8	Critical Critical	Both on March 17th, 2020	Apex One, OfficeScan

Details of the vulnerability

CVE-2020-8467 is a critical remote code execution vulnerability in the migration tool component of Trend Micro Apex One and OfficeScan. CVE-2020-8468 is a high severity content validation escape vulnerability in Trend Micro Apex One and OfficeScan agents. This bug allows an attacker to manipulate certain agent client components.

Trend Micro released a total of five patches including the above-mentioned CVEs in its security advisory of March. All of them are critical, and the two CVEs mentioned in the previous paragraph were zero-day vulnerabilities exploited in the wild. More about the vulnerabilities **here.**

Impact

The exploitation of these critical vulnerabilities could allow attackers to execute arbitrary code, bypass security mechanisms and modify sensitive components on target systems.

Solution

Trend Micro released a security advisory with patches for all five vulnerabilities.

Victims

On June 28th, 2019, Mitsubishi Electric, a Japanese electronics vendor and defense contractor detected an intrusion in its network. The company issued a press release saying files containing information about 1,987 employees were stolen. They also lost some confidential technical and sales materials.

06 VULNERABILITIES IN SALTSTACK SALT

CVEs	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-11651 CVE-2020-11652	9.8 6.5	Critical Medium	May 19th, 2020	SaltStack Salt before 2019.2.4 and 3000 before 3000.2

Details of the vulnerability

SaltStack Salt is an open-source remote task and configuration management framework widely used in data centers and cloud environments. Two flaws were found in Salt's ZeroMQ protocol (used for master-slave communication) in the master-slave architecture. More about the vulnerabilities **here.**

Impact

The exploitation of these vulnerabilities could allow attackers to execute arbitrary commands on the target systems.

Solution

SaltStack released security fixes to mitigate these vulnerabilities in Salt.

Victims

Both Ghost, a content management platform, and Xen Orchestra, an orchestration platform for Xen servers, were hit by the attacks. The **companies** did not announce theft of sensitive data, but some of their services were unavailable for a period of time. **Lineage OS Project,** had to take down multiple servers to deal with the attack.

07 NXNS ATTACK ON DNS SERVERS

CVE	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-8616 CVE-2020-12662 CVE-2020-10995 CVE-2020-12667	8.6 7.5 7.5 7.5	Critical High High High	May 19th, 2020	DNS servers (Bind, Microsoft DNS, CloudFlare, Google, PowerDNS, etc.)

Details of the vulnerability

A team of Israeli researchers discovered these vulnerabilities in the global architecture of DNS servers. The flaws exist in the DNS protocol and affect all recursive DNS resolvers.

An attacker could mount DDOS (Distributed Denial of Service) attacks, dubbed as NSNX (Non-eXistent Name Servers Attack) attacks against both recursive resolvers and authoritative servers and cause massive disruption in global internet traffic until websites are forced to go offline. More details about the vulnerabilities **here.**

Impact

An attacker could mount DDOS attacks against both recursive resolvers and authoritative servers and cause massive disruption in global internet traffic until websites are forced to go offline.

Victims

There is no evidence about the exploitation of these vulnerabilities.

Solution

The Israeli researchers said they've been working for the past few months with the makers of DNS software, content delivery networks, and managed DNS providers to apply mitigations to DNS servers across the world. Server administrators who run their own DNS servers can update their DNS resolver software to the latest version.

08 RIPPLE20 VULNERABILITIES IN IOT DEVICES

CVEs	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-11896 CVE-2020-11897 CVE-2020-11898 CVE-2020-11901 15 more.	10.0 10.0 9.1 9.0 etc.	Critical	June 17th, 2020	TCP/IP Stack

Details of the vulnerability

A total of 19 critical and high-severity vulnerabilities were discovered by an Israeli research team in a low-level TCP/IP software library. There are four critical vulnerabilities in Treck TCP/IP stack, with CVSS scores more than 9. If an attacker weaponizes these vulnerabilities, it could allow the perpetrator to gain complete control over targeted devices without requiring any user interaction.

All these vulnerabilities exist in connected devices offered by various companies including Schneider Electric, Caterpillar, Cisco, HP, Intel, Rockwell Automation, among others. Affected hardware includes everything from connected printers to medical infusion pumps and industrial-control gear. More about the vulnerabilities **here.**

Impact

The exploitation of these vulnerabilities could allow attackers for remote code execution, denial-of-service (DoS) attacks, and obtain potentially sensitive information.

Victims

There is no evidence about the exploitation of these vulnerabilities.

Solution

Treck has issued a patch for use by OEMs in a newer Treck stack version (6.0.1.67 or higher). Tech giants like Intel, HP, Schneider Electric, Caterpillar, B.Braun, Green Hills, Rockwell Automation, and Cisco have also released their advisories.

09 CRITICAL VULNERABILITIES IN ZOOM

CVEs	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-6109 CVE-2020-6110	9.8 8.8	Critical High	June 8th, 2020	Zoom Client Application prior to 4.6.12

Details of the vulnerability

CVE-2020-6109 is a flaw that can be exploited using GIF messages. Zoom displays the GIF in chat by fetching it via an HTTP URL. Since no validation is performed, URLs can point to arbitrary locations and leak the client's unique ID. CVE-2020-6110 is a flaw than can be exploited using zip files. When a client receives a malicious zip file, Zoom does not validate the file. When a file with malicious code is opened, the contents are not just unzipped without verifying, but also to a directory as specified by the attacker. More details about the vulnerabilities **here.**

Impact

Attackers can exploit these critical vulnerabilities to execute arbitrary code by exploiting a directory traversal vulnerability.

Victims

Many users across business meetings, educational institutions, support groups, etc. have complained about 'zoom-bombings' where bad actors enter a video call and disrupt meetings by giving threats or performing unwanted actions in the app.

Solution

Both the vulnerabilities were addressed in Zoom 4.6.12. Upgrading to the mentioned version will fix the vulnerabilities.

10 SMBLEED AND SMBGHOST VULNERABILITIES IN WINDOWS SMB PROTOCOL

CVEs	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-1206 CVE-2020-0796	7.5 10.0	High Critical	June 9th, 2020 March 12th, 2020	Windows SMBv3

Details of the vulnerability

The Server Message Block Protocol (SMB protocol) which runs over TCP port 445 is a client-server communication protocol used for sharing access to files, printers, network browsing, and inter-process communication over a network.

The SMBleed (CVE-2020-1206) vulnerability in SMB protocol could allow attackers to leak kernel memory remotely. When combined with a previously disclosed wormable SMBGhost vulnerability (CVE-2020-0796), attackers can perform remote code execution (RCE) to gain control over the server or client. More about the vulnerabilities **here.**

Impact

The exploitation of these vulnerabilities could allow remote attackers to access sensitive information or execute arbitrary code on the target systems with unpatched SMBv3 server/client.

Solution

Microsoft has released security updates for both vulnerabilities in the Patch Tuesday updates of March and June.

Victims

Netwalker ransomware group exploited the SMBGhost vulnerability (along with a few other vulnerabilities) to hack into the network of **Michigan State University**. They stole financial data and threatened to leak them publicly if the demanded ransom was not paid.

11 SIGRED VULNERABILITY IN WINDOWS DNS SERVER

CVEs	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-1350	10.0	Critical	June 14th, 2020	Windows DNS servers

Details of the vulnerability

This is a 17-year-old wormable flaw discovered in Windows DNS servers. The flaw was found in how DNS Server parses incoming query or a response for a forwarded request. When an attacker sends malicious queries to the server, a buffer overflow occurs and lets the attacker execute remote code on the target server. Microsoft has warned that the vulnerability will also be found in Windows servers that have been configured as DNS servers. Some security researchers even commented on the vulnerability as “more than just another vulnerability”. Additional details **here.**

Impact

An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the local system account.

Solution

Microsoft released a security update to fix this vulnerability in Patch Tuesday of July 2020.

Victims

There is no evidence about exploitation of this vulnerability although it has been around for 17 years.

12 CRITICAL VULNERABILITY IN F5 BIG-IP DEVICES

CVE	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-6902	9.8	Critical	July 1st, 2020	BIG-IP Devices (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) versions 11.6.x prior to 11.6.5.2, 12.1.x prior to 12.1.5.2, 13.x prior to 13.1.3.4, 14.x prior to 14.1.2.6 and 15.x prior to 15.1.0.4.

Details of the vulnerability

The vulnerability resides in the configuration interface, also referred as Traffic Management User Interface (TMUI), of the BIG-IP application delivery controller (ADC). An attacker just needs to send a specifically crafted HTTP request to the server hosting the Traffic Management User Interface (TMUI) utility for BIG-IP configuration. More about the vulnerability **here.**

Impact

This vulnerability allows an attacker to create or delete files, disable services, intercept information, run arbitrary system commands and Java code, completely compromise the system, directory traversal exploitation and pursue further targets, such as the internal network.

Solution

F5 has released security fixes for these vulnerabilities. Upgrade BIG-IP Devices to the latest of their corresponding versions. 11 series to 11.6.5.2, 12 series to 12.1.5.2, 13 series to 13.1.3.4, 14 series to 14.1.2.6, 15 series to 15.1.0.4.

Victims

There is no evidence about the exploitation of this vulnerability. However, The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an **alert** about the active exploitation of the unauthenticated remote code execution (RCE) CVE-2020-5902 vulnerability affecting F5 Big-IP ADC devices.

13 HIGH-RISK VULNERABILITY IN TEAMVIEWER

CVE	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-13699	8.8	High	July 29th, 2020	TeamViewer for Windows prior to 8.0.258861, 9.0.258860, 10.0.258873, 11.0.258870, 12.0.258869, 13.2.36220, 14.2.56676, 14.7.48350, and 15.8.3.

Details of the vulnerability

The vulnerability is a security flaw that stems from an unquoted search path or element. Specifically, this vulnerability is due to the application not correctly quoting its custom URI handlers. A user with an installed vulnerable TeamViewer version is tricked into visiting a maliciously crafted website to exploit this vulnerability.

Successful exploitation of this vulnerability could allow a remote attacker to launch TeamViewer with arbitrary parameters. The application could be forced to relay an NTLM authentication request to the attacker's system enabling offline rainbow table attacks and brute force cracking attempts. Read more about the vulnerability **here.**

Impact

The exploitation of the vulnerability could allow remote attackers to obtain sensitive credential information or take full control over the affected system.

Victims

There is no evidence about the exploitation of this vulnerability.

Solution

TeamViewer has released a security update to fix this vulnerability.

14 CRITICAL BOOTHOLE VULNERABILITY IN GRUB2 BOOTLOADER

CVE	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-10713	8.2	High	July 30th, 2020	GRUB2 version 2.06 and prior, Linux systems, Windows 8.1, 10, Server 2012, Server 2016, Server 2019

Details of the vulnerability

This vulnerability termed "Hole in the Boot" allows an attacker to load a malicious kernel instead. Once the attacker has physical or remote access to the system within the same network, they can craft a string as a malicious payload that causes a buffer overflow, leading to the execution of arbitrary code. This vulnerability instilled additional efforts to audit the GRUB2 bootloader and led to the discovery of six more vulnerabilities. More about the vulnerabilities **here.**

Impact

Attackers can exploit these critical vulnerabilities to execute arbitrary code and bypass Secure Boot restrictions.

Victims

There is no evidence about the exploitation of these vulnerabilities. Although millions of enterprise devices are at serious risk.

Solution

Linux and Windows have released security updates to fix the vulnerability.

15 ZEROLOGON VULNERABILITY IN WINDOWS DOMAIN CONTROLLER

CVE	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-1472	10.0	Critical	August 17th, 2020	Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2008 R2 Service Pack 1.

Details of the vulnerability

The Netlogon Remote Protocol is an RPC interface available on Windows domain controllers which is used to facilitate the authentication between users and machines, especially to the users logging in to the servers using NTLM (NT LAN Manager) protocol.

The vulnerability in the Netlogon Remote Protocol of the Windows server allows an unauthenticated user to a compromise the domain controller of active directory services and gain admin privileges. More about the vulnerability **here.**

Impact

An attacker who successfully exploited the vulnerability can take over the domain controller and run a specially crafted application on any device on the network.

Solution

Microsoft released a security update to fix this vulnerability in Patch Tuesday of August 2020.

Victims

The Cybersecurity Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) reported risks to election support systems and critical infrastructure. The attacks were directed at but not limited to federal and state, local, tribal, and territorial (SLTT) government networks.

16 CRITICAL RCE FLAWS IN ORACLE WEBLOGIC SERVER

CVE	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-14750 CVE-2020-14882	9.8 9.8	Critical Critical	November 2nd, October 21st, 2020	Oracle WebLogic Server versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, and 14.1.1.0.0

Details of the vulnerability

Oracle released a special advisory pointing out a flaw in the console component of Oracle WebLogic server that could be exploited via a HTTP protocol. The patch fix for this vulnerability is believed to be a bypass for the patch released for **CVE-2020-14882**, a similar remote code execution flaw that is being exploited by DarkIRC botnet. More about the vulnerability (CVE-2020-14750) **here.**

Impact

The vulnerability could be exploited without any user interaction and credentials to execute arbitrary code on the affected system.

Solution

Oracle has released security updates to fix these vulnerabilities.

Victims

DarkIRC botnet is actively targeting thousands of Oracle WebLogic servers to exploit the vulnerability.

17 TWO CRITICAL ZERO-DAY VULNERABILITIES IN GOOGLE CHROME

CVEs	CVSS 3.0	Severity	Disclosed on	Affected Products
CVE-2020-16013 CVE-2020-16017	8.8 9.6	High Critical	November 12th, 2020	Google Chrome versions before 86.0.4240.198.

Details of the vulnerability

The vulnerability CVE-2020-16013 exists in the V8 JavaScript rendering engine, it is the component of chrome that handles JavaScript code. CVE-2020-16017 is a use-after-free memory corruption issue in Google Chrome's site isolation feature. It is the component of chrome which isolates each site's data from one and another. More about the vulnerabilities **here.**

Impact

These vulnerabilities allow attackers to cause a program to crash, use unexpected values, or execute code on the affected system.

Victims

There is no evidence about the victims although Google has received reports regarding the exploitation of this vulnerability.

Solution

Google has released the security updates addressing the issue in Google Chrome version 86.0.4240.198.

18 APPLE SECURITY UPDATES DECEMBER 2020

CVEs	Severity	Disclosed on	Affected Products
70+ CVEs	Critical	December 14th,2020	Multiple versions of macOS, macOS server, iOS, iPadOS, Safari, tvOS, watchOS

Details of the vulnerability

Apple released security updates for vulnerabilities in multiple products. macOS had fixes for 59 vulnerabilities with various impacts ranging from reading arbitrary files to code execution. An improper input validation issue existed in the parsing of URLs of the macOS Server. The flaw could be used by an attacker to conduct open redirect or cross-site scripting attacks. A use-after-free vulnerability was fixed in Apple Safari. Processing of maliciously crafted web content may allow attackers to launch arbitrary code execution. More about the vulnerabilities **here.**

Impact

The disclosed vulnerabilities could cause many impacts such as open redirection, cross-site scripting, arbitrary code execution, authentication bypass, information disclosure, memory corruption, and more.

Solution

Apple has released security updates for all the vulnerabilities.

19 MOZILLA PATCH FIXES FOR ONE ZERO-DAY AND 15+ HIGH-SEVERITY VULNERABILITIES

CVEs	Severity	Disclosed on	Affected Products
CVE-2020-15999 (zero-day), 15+ CVEs	Critical	November 22nd,2020	Firefox before version 83, Firefox ESR before version 78.5, Thunderbird before version 78.5

Details of the vulnerability

Mozilla released security updates to address vulnerabilities along with a 'https only' feature to covert http to https automatically in Firefox version 83. The zero-day is a heap buffer overflow vulnerability that can be triggered by embedding PNG images into fonts. The bug could only be exploited if a rarely used, hidden preference is toggled. It only affects the Linux and Android operating systems. More about the other high severity vulnerabilities **here.**

Impact

The vulnerabilities can cause heap buffer overflow, application crash, memory corruption, and more.

Victims

There is no evidence about the exploitation of these vulnerabilities.

Solution

Mozilla has released security updates for all the vulnerabilities.

20 SOLARWINDS SECURITY UPDATES TO PREVENT EXPLOITS BY SUPERNOVA MALWARE

CVEs	CVSS 3.0	Severity	Disclosed on
CVE-2020-10148	9.8	Critical	December 27th,2020
CVE-2020-14005	8.8	High	June 24th,2020
CVE-2020-13169	9.6	Critical	September 17th,2020

Affected Products

Application Centric Monitor, Database Performance Analyzer Integration Module, Enterprise Operations Console, High Availability, IP Address Manager, Log Analyzer, Network Automation Manager, Network Configuration Manager, Network Operations Manager, User Device Tracker, Network Performance Monitor, NetFlow Traffic Analyzer, Server & Application Monitor, Server Configuration Monitor, Storage Resource Monitor, Virtualization Manager, VoIP & Network Quality Manager, Web Performance Monitor (WPM)

Details of the vulnerability

The SolarWinds Orion API is used to interface with all SolarWinds Orion Platform products. The vulnerability resides in the SolarWinds Orion API, making it vulnerable to an authentication bypass that can further lead to remote code execution. The vulnerability can be used to deploy SUPERNOVA malware on the target environment. SolarWinds was also the victim of a highly sophisticated breach and malware attack called **SUNBURST.** More about the vulnerability **here.**

CVE-2020-13169 is a HTML injection vulnerability in the SolarWinds Orion Platform. It could lead to information disclosure and escalation of privileges by admin takeover. CVE-2020-14005 is a vulnerability due to a visual basic script that could lead to remote code execution.

Impact

The vulnerabilities could allow remote attackers to bypass authentication, escalate privileges, and execute remote code.

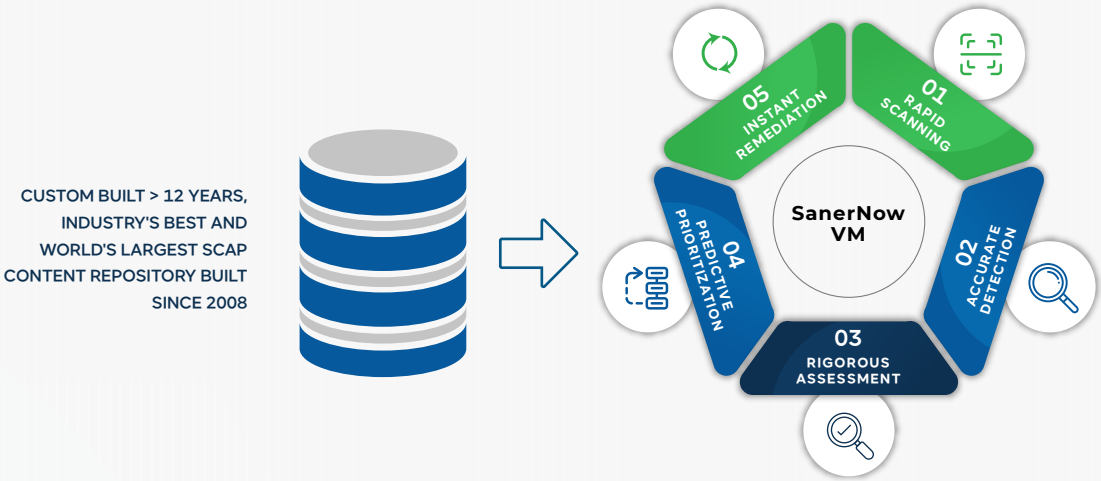
Solution

SolarWinds has released security updates to patch these vulnerabilities. Upgrade SolarWinds products to their latest versions to keep your systems secure.

Victims

The SUNBURST attack was a global intrusion campaign across many locations. Multiple government, consulting, technology, telecom, and extractive entities in North America, Europe, Asia, and Middle East are victims of this attack.

SANERNOW VULNERABILITY MANAGEMENT:
YOUR PARTNER TO FIGHT THE VULNERABILITIES OF 2021



The number of reported vulnerabilities has risen by a whopping **183 percent** in the last 5 years (2015-2020). The total number of vulnerabilities in 2020 was the highest ever with 18,355 vulnerabilities, beating the previous year's record. Vulnerability management is growing in complexity year on year and managing risks is getting more challenging with growing remote workforces across organizations.

SanerNow Vulnerability Management is a cloud-based tool to scan, detect, assess, prioritize, and mitigate vulnerabilities. It can help you:

- Perform the most comprehensive vulnerability scans by leveraging our homegrown, world's largest vulnerability database with over 100,000 security checks
- Run the fastest vulnerability scans across entire networks in under 5 minutes
- Keep a keen eye on new vulnerabilities in your environment with real-time continuous scanning
- Mitigate the vulnerabilities with integrated patch management that lets you deploy patches and track your vulnerability management to completion.
- Assess and prioritize vulnerabilities accurately based on the true risk levels to your specific environment

During such a paradigm shift in IT security and management, a more comprehensive and stronger approach to vulnerability management will equip you to take on the challenges of 2021 with confidence.

Schedule a Demo

We'll show you SanerNow Vulnerability Management in action.