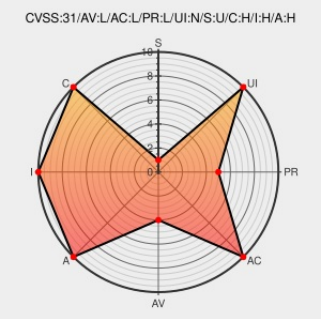
CVE-2020-24556

Published on: 09/01/2020 12:00:00 AM UTC

Last Modified on: 04/28/2022 06:28:00 PM UTC

CVE-2020-24556

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Macos from Apple contain the following vulnerability:

A vulnerability in Trend Micro Apex One, OfficeScan XG SP1, Worry-Free Business Security 10 SP1 and Worry-Free Business Security Services on Microsoft Windows may allow an attacker to create a hard link to any file on the system, which then could be manipulated to gain a privilege escalation and code execution. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected.

CVE-2020-24556 has been assigned by security@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Trend Micro** - **Trend Micro Apex One** version **2009 (on premise), SaaS**

Affected Vendor/Software: **Trend Micro** - **Trend Micro OfficeScan** version **XG SP1**

Affected Vendor/Software: **Trend Micro** - **Trend Micro Worry-Free Business Security** version **10 SP1, Services (SaaS)**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

Impact	Impact	Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SECURITY BULLETIN: August 2020 Security Bulletin for Trend Micro Apex One and Apex One as a Service	Vendor Advisory success.trendmicro.com text/html	MISC success.trendmicro.com/solution/000263632
ZDI-20-1093 | Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-20-1093/
SECURITY BULLETIN: September 2020 Security Bulletin for Trend Micro Worry-Free Business Security and Worry-Free Business Security Services	success.trendmicro.com text/html	MISC success.trendmicro.com/solution/000267260
SECURITY BULLETIN: Trend Micro OfficeScan XG Hard Link Privilege Escalation Vulnerability	Vendor Advisory success.trendmicro.com text/html	MISC success.trendmicro.com/solution/000263633

Related QID Numbers

375757 Trend Micro Apex One(On-Prem) Multiple Vulnerabilities(000263632)(August 2020)

375758 Trend Micro OfficeScan XG Hard Link Privilege Escalation Vulnerability(000263632)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Trendmicro	Apex One	2019	All	All	All
Application	Trendmicro	Apex One	saas	All	All	All
Application	Trendmicro	Apex One	2019	All	All	All
Application	Trendmicro	Apex One	saas	All	All	All
Application	Trendmicro	Worry-free Business Security	10.0	sp1	All	All
Application	Trendmicro	Worry-free Business Security Services	-	All	All	All

cpe:2.3:o:apple:macos:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:apex_one:2019:*:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:apex_one:saas:*:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:apex_one:2019:*:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:apex_one:saas:*:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:worry-free_business_security:10.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:worry-free_business_security_services:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→