Vulnerability discovered in ESET anti-virus software could allow hackers to gain system privileges on Windows

This vulnerability, with a tracking identifier of CVE-2021-37852, was first reported by security researcher Michael DePlante from the Trend Micro team.

The well-known internet security company ESET has urgently released a series of patches to completely address a high-severity local security vulnerability that affects many ESET antivirus software products running on Windows computers. Windows 10 or Windows Server 2016 or later systems worldwide.

This vulnerability, with a tracking identifier of CVE-2021-37852, was first reported by security researcher Michael DePlante from the Trend Micro team. According to the analysis results, this is considered an extremely dangerous vulnerability because it allows attackers to take over and upgrade privileges to the NT AUTHORITYSYSTEM account (the highest privilege level on Windows systems). by abusing Windows Antimalware Scan Interface (AMSI).

AMSI was first introduced with Windows 10 Technical Preview in 2015. It is a tool designed to allow applications and services to request a memory cache scan from any major anti-virus software installed. installed on the system.

According to ESET, the danger can only appear after attackers gain SeImpersonatePrivilege permissions, which are usually assigned to users in the Local Administrators group and the Local Service account. of the device to impersonate a client after authentication. This will "limit the impact of this vulnerability". This somewhat limits the impact of the vulnerability in practice.

However, the warning from ZDI states that attackers also only need to "gain the ability to execute low-privileged code on the target system" to abuse the vulnerability. This is consistent with ESET's CVSS severity rating, and also shows that the vulnerability can be exploited by low-privileged threat actors.

Affected ESET products

The list of ESET software products affected by this vulnerability is quite long, including:

1. ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security and ESET Smart Security Premium from versions 10.0.337.1 to 15.0.18.0.
2. ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows from versions 6.6.2046.0 to 9.0.2032.4.
3. ESET Server Security for Microsoft Windows Server 8.0.12003.0 and 8.0.12003.1, ESET File Security for Microsoft Windows Server from versions 7.0.12014.0 to 7.3.2006.0.
4. ESET Server Security for Microsoft Azure from version 7.0.12016.1002 to 7.2.12004.1000.
5. ESET Security for Microsoft SharePoint Server from version 7.0.15008.0 to 8.0.15004.0.
6. ESET Mail Security for IBM Domino from version 7.0.14008.0 to 8.0.14004.0.
7. ESET Mail Security for Microsoft Exchange Server from version 7.0.10019 to 8.0.10016.0.

ESET Server Security for Microsoft Azure users are also advised to immediately update ESET File Security for Microsoft Azure to the latest available version of ESET Server Security for Microsoft Windows Server to resolve the issue.

ESET has released multiple security updates between December 8 and January 31 to address this vulnerability. This is quite a remarkable effort. Fortunately, ESET has not (yet) found any evidence of the vulnerability being exploited in the wild.

> "The attack surface can also be eliminated by disabling the Enable advanced scanning via AMSI option in the Advanced Setup of ESET products. However, we strongly recommend that you perform the upgrade to the product version. fixed product and only apply this solution when it is not possible to update to the new version for some important reason,' the warning from ESET said.