ESET antivirus bug let attackers gain Windows SYSTEM privileges

By
Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)

February 2, 2022 05:00 PM **0**

Image: ESET

Slovak inter
severity loca
systems run

law (CVE-2021-37852 (https://cve.mitre.org/cgi-bin/cvename.cgi?

AUTHORITY\SYSTEM account rights (the highest level of privileges on a Windows system) using the Windows Antimalware Scan Interface (AMSI).

AMSI (https://docs.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal) was first introduced with Windows 10 Technical Preview in 2015 (http://cloudblogs.microsoft.com/microsoftsecure/2015/06/09/windows-10-to-offer-application-developers-new-malware-defenses/), and it allows apps and services to request memory buffer scans from any major antivirus product installed on the system.

According to ESET (https://support.eset.com/en/ca8223-local-privilege-escalation-vulnerability-fixed-in-eset-products-for-windows), this can only be achieved after attackers gain SeImpersonatePrivilege rights (https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/seimpersonateprivilege-secreateglobalprivilege), normally assigned to users in the local Administrators group and the device's local Service account to impersonate a client after authentication which should "limit the impact of this vulnerability."

However, ZDI's advisory (https://www.zerodayinitiative.com/advisories/ZDI-22-148/) says attackers are only required to "obtain the ability to execute low-privileged code on the target system," which matches ESET's CVSS severity rating (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H&version=3.1) also showing that the bug can be exploited by threat actors with low privileges.

While ESET said it only found out about this bug on November 18, a disclosure timeline available in ZDI's advisory reveals that the vulnerability was reported four months earlier, on June 18, 2021.

- ESET Server Security for Microsoft Windows Server 8.0.12003.0 and 8.0.12003.1, ESET File Security for Microsoft Windows Server from version 7.0.12014.0 to 7.3.12006.0
- ESET Server Security for Microsoft Azure from version 7.0.12016.1002 to 7.2.12004.1000
- ESET Security for Microsoft SharePoint Server from version 7.0.15008.0 to 8.0.15004.0
- ESET Mail Security for IBM Domino from version 7.0.14008.0 to 8.0.14004.0
- ESET Mail Security for Microsoft Exchange Server from version 7.0.10019 to 8.0.10016.0

Users of ESET Server Security for Microsoft Azure are also advised (https://support.eset.com/en/kb3748-upgrade-eset-file-security-for-microsoft-azure-to-the-latest-version-of-eset-server-security-for-microsoft-windows-server) to immediately update ESET File Security for Microsoft Azure to the latest available version of ESET Server Security for Microsoft Windows Server to address the flaw.

The antivirus maker released multiple security updates between December 8 and January 31 (https://support.eset.com/en/ca8223-local-privilege-escalation-vulnerability-fixed-in-eset-products-for-windows) to address this vulnerability, when it patched the last vulnerable product exposed to attacks.

Luckily, ESET found no evidence of exploits designed to target products affected by this security bug in the wild.

"The attack surface can also be eliminated by disabling the Enable advanced scanning via AMSI option in ESET products' Advanced setup," ESET added.

"However, ESET strongly recommends performing an upgrade to a fixed product version and only applying this workaround when the upgrade is not possible for an important reason."