Authentication bypass misconfiguration in the RADIUS component of ESET Secure Authentication

2025-05-26 - Steef | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2025-0007

May 23, 2025

Severity: High

Summary

An internal investigation, based on a report from a customer, revealed a possible misconfiguration in the RADIUS component of ESET Secure Authentication. Please note that the flaw was present in the single component of ESET Secure Authentication, not the platform as a whole and was exploitable only through the use of **incorrect RADIUS client configuration.** The misconfiguration allowed an attacker to create user accounts in ESET Secure Authentication (cloud version) without having proper permissions to do so. This led to a possible authentication bypass for resources that are allowed by the administrator to be accessed without 2FA verification.

ESET released a preventive measure for this issue on February 19, 2025. We strongly recommend that ESET Secure Authentication administrators take mitigation steps detailed in the Solution section below.

This abovementioned misconfiguration is not possible in ESET Secure Authentication On-Prem deployments with default authentication settings, namely when the corresponding setting is selected:

RADIUS client (e.g., VPN)	ESET Secure Authentication On-Prem – RADIUS Server setting
First-factor authentication (password verification) performed on the RADIUS client	Client validates username and password
First-factor authentication (password verification) NOT performed on the RADIUS client	Client does not validate username and password

Note

Listed combinations are simplified; for further details, refer to our Online Help documentation.

Details

The misconfiguration may have caused issues for the following combination of settings:

- The customer used a RADIUS client (for example, a VPN) that does not perform first-factor authentication (password verification)
- An incorrectly set RADIUS Server setting in the ESET Secure Authentication Web Console's settings to either "Client validates username and password" or "Client validates username and password – use Access-Challenge"
- Components → selected component → Allow non-2FA: enabled

Important!

Please note that the cloud version of ESET Secure Authentication does not offer a Client Type option: "Client does not validate username and password".

For further details, refer to our Online Help documentation.

The misconfiguration, together with the RADIUS “auto-registration” feature, led to the RADIUS server allowing unintended user account creation even when the feature was disabled for other components. This led to the CWE-863 Incorrect Authorization problem type, finally causing CAPEC-115 Authentication Bypass, if first-factor authentication (password verification) was not enforced on the RADIUS client (note that such configuration is not supported in the cloud version) and also non-2FA users were allowed in the RADIUS component configuration. An attacker could possibly attempt to log in with a random password and potentially gain access to RADIUS clients protected by the ESA RADIUS component that do not require the 2FA verification.

Solution

ESET released an update to version 4.12.1.0 of ESET Secure Authentication (cloud) on February 19, 2025, which disables the auto-registration feature for the RADIUS component to prevent a security risk even in the case of an incorrect RADIUS client configuration. This version has already been deployed to all customers, as the upgrades are managed centrally by ESET.

We strongly recommend that ESET Secure Authentication administrators:

1. Perform an audit of the authentication settings and enforce first-factor authentication (password verification) on the RADIUS clients.

2. Perform a check of the accounts created in ESET Secure Authentication and remove the accounts that should not have access to the protected resources.

Affected products

- ESET Secure Authentication

Feedback & Support

If you have feedback or questions about this issue, contact us via the ESET Security Forum or via local ESET Technical Support.

Version log

- Version 1.0 (May 23, 2025): Initial version of this document