Security advisory: command injection vulnerability (CVE-2025-59689)

Description

Libraesva ESG is affected by a command injection flaw that can be triggered by a malicious e-mail containing a specially crafted compressed attachment, allowing potential execution of arbitrary commands as a non-privileged user. This occurs due to an improper sanitization during the removal of active code from files contained in some compressed archive formats.

The vulnerability affects versions of Libraesva ESG starting from version 4.5.

For ESG 5.0 a fix has been released in 5.0.31
For ESG 5.1 a fix has been released in 5.1.20
For ESG 5.2 a fix has been released in 5.2.31
For ESG 5.3 a fix has been released in 5.3.16
For ESG 5.4 a fix has been released in 5.4.8
For ESG 5.5. a fix has been released in 5.5.7

The fixes have been released through the automatic updates channel.

Versions below 5.0 are EOS and must be manually upgraded.

Libraesva cloud customers

All appliances in Libraesva cloud have been upgraded to the latest version containing the fix. No further action needed.

Libraesva on-premise customers

All on-premise appliances with versions 5.X have been automatically upgraded to the latest version containing the fix as confirmed by our telemetry data.

On-premise customers of version 5.X appliances can verify the current installed version in the

admin dashboard.

On-premise customers with 4.X versions, which are in End Of Support, must manually upgrade to 5.x.

Vulnerability overview

Trigger mechanism

An attacker can exploit this flaw by sending an e-mail that contains a specially crafted compressed archive. The vulnerability is only triggered with specific archive formats. Within the archive, the payload files are constructed to manipulate the application's sanitization logic, exploiting an improper sanitization of input parameters.

Impact

Once the sanitization bypass is achieved, the attacker can execute arbitrary shell commands under a non-privileged user account.

Known Exploitation

One confirmed incident of abuse has been identified. The threat actor is believed to be a foreign hostile state entity.

Remediation timeline

Discovery to Fix Deployment: 17 hours
Remediation Action: Libraesva released an emergency, automated patch to all ESG 5.x installations (both cloud and on-prem).
Patch Contents:

1. Core fix to correct the sanitization flaw.
2. Automated scan for compromise indicators of compromise (IoCs).
3. Self-assessment module that runs on all affected appliances (cloud and on-prem) to verify patch integrity and detect residual threats.

The single-appliance focus underscores the precision of the threat actor (believed to be a

foreign hostile state) and highlights the importance of rapid, comprehensive patch deployment.