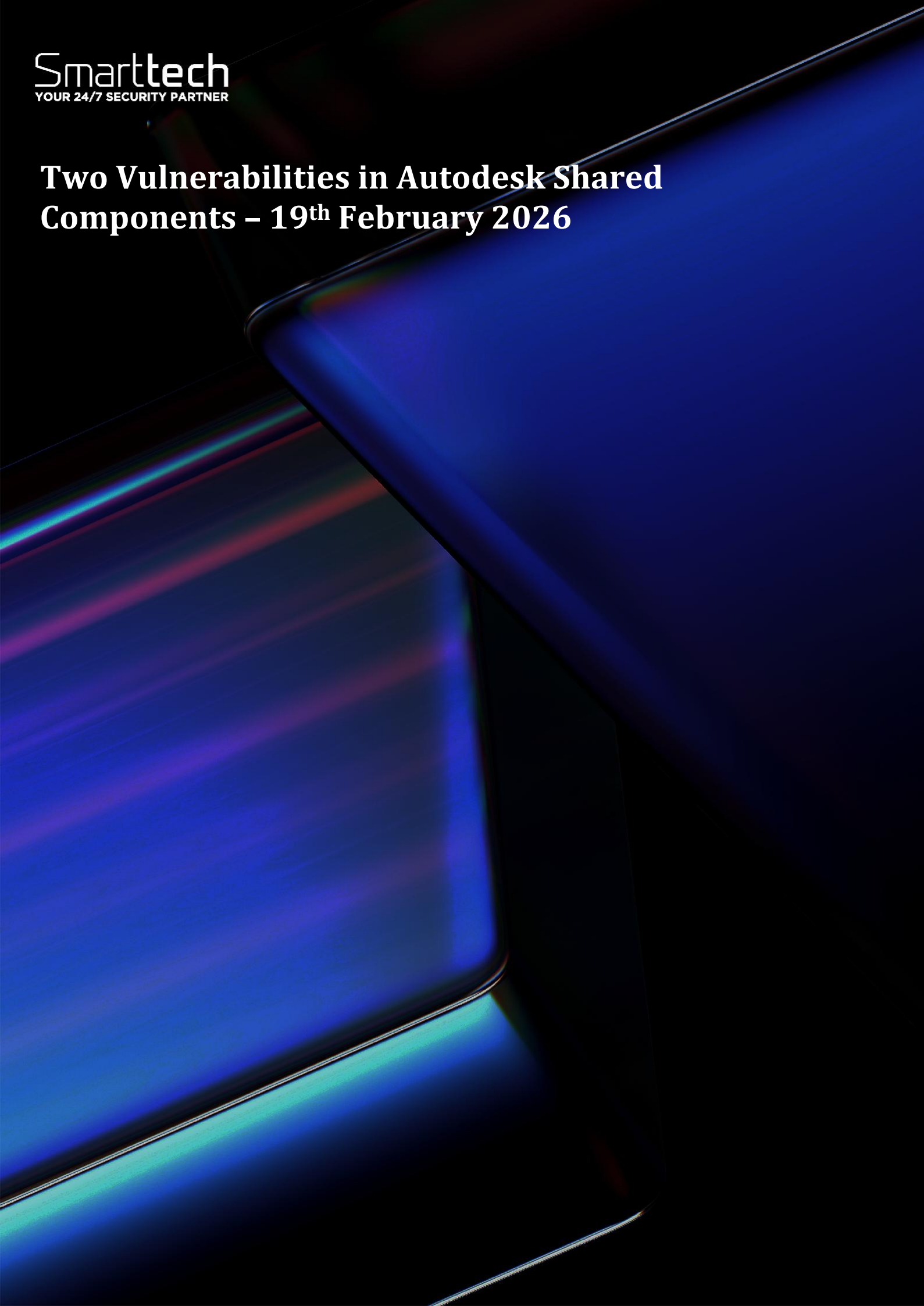
Smarttech
YOUR 24/7 SECURITY PARTNER

Two Vulnerabilities in Autodesk Shared Components – 19th February 2026



Document ID	SMA-Informative Cyber Alert
Document status	ISSUED
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	19th February 2026
Issue Date	19th February 2026

Informative Cyber Alerts are reports created by Smarttech247 designed to inform customers about medium and low severity vulnerabilities, IOCs from certain attacks/breaches, and other information that could help companies be aware and protect against any attack.
The content of this report should be regarded as simply informative as it usually addresses products that have an auto-update option available for patches. It will be the customer's decision if it is necessary to follow any recommendation or disregard them as they are not currently applicable in the environment.

Overview

Two vulnerabilities found in Autodesk Shared Components could allow remote attackers to execute arbitrary code. User interaction is required for exploitation, as the target must open or run a maliciously crafted file. These specific flaws exist within the parsing of maliciously crafted CATPART and MODEL files that can force an Out-of-Bounds Write vulnerability.

Technical Summary

Details of these vulnerabilities are as follows:

CVE	CVE Score	Description
CVE-2026-0874	7.8	A maliciously crafted CATPART file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.
CVE-2026-0875	7.8	A maliciously crafted MODEL file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.

Note: *The VPR scores are not available at this moment. Also, there are currently no reports of these vulnerabilities being exploited in the wild.*

Affected Products

Impacted Versions	Mitigated Versions
Autodesk Shared Components 2026.5 or earlier	Autodesk Shared Components 2026.6

Recommendations

Smarttech247 team recommends the following actions to be taken:

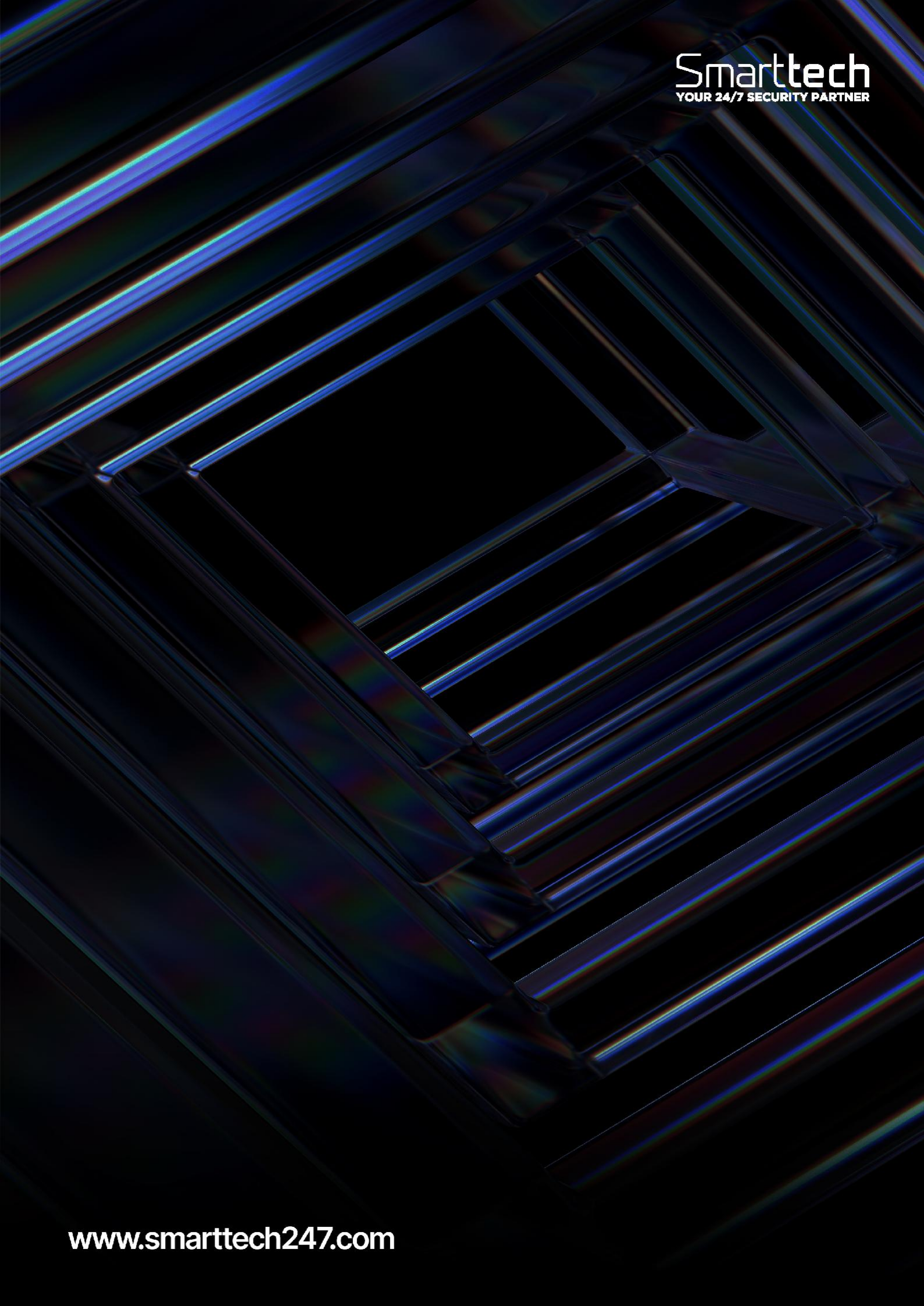
- Upgrade to the latest versions from vendor's website in order to obtain a fix for these vulnerabilities.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.

References

https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0004
https://www.autodesk.com/products/autodesk-access/overview
https://manage.autodesk.com/

CVE

CVE-2026-0874
CVE-2026-0875


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com