SECURITYWEEK NETWORK:

- Cybersecurity News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2021 CISO Forum
- ICS Cyber Security Conference
- Contact

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance

- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response

- ICS/OT
- IoT Security

Home › Cloud Security

Microsoft Informs Users of High-Severity Vulnerability in Azure AD

By Ionut Arghire on November 18, 2021

Microsoft on Wednesday informed customers about a recently patched information disclosure vulnerability affecting Azure Active Directory (AD).

Tracked as CVE-2021-42306 (CVSS score of 8.1), the vulnerability exists because of the manner in which Automation Account “Run as” credentials are created when a new Automation Account is set up in Azure.

Due to a misconfiguration in Azure, Automation Account “Run as” credentials (PFX certificates) ended up being stored in clear text in Azure AD and could be accessed by anyone with access to information on App Registrations. An attacker could use these credentials to authenticate as the App Registration.

Security researchers with enterprise penetration testing firm NetSPI, who identified the vulnerability, explain that an attacker could leverage the bug to escalate privileges to Contributor of any subscription that has an Automation Account, and access resources in the affected subscriptions.

“This includes credentials stored in key vaults and any sensitive information stored in Azure services used in the subscription. Or worse, they could disable or delete resources and take entire Azure tenants offline,” the researchers explain.

According to Microsoft, the vulnerability is related to the keyCredentials property, which was designed for configuring authentication credentials for applications, and which accepts a certificate containing public key data for authentication, but which also incorrectly stored such certificates.

“Some Microsoft services incorrectly stored private key data in the (keyCredentials) property while creating applications on behalf of their customers. We have conducted an investigation and have found no evidence of malicious access to this data,” Microsoft says.

The tech giant says it has addressed the bug by preventing Azure services from storing clear text private keys in the keyCredentials property and by preventing users from reading any private key data that has been incorrectly stored in clear text.

“As a result, clear text private key material in the keyCredentials property is inaccessible, mitigating the risks associated with storage of this material in the property,” the company says.

Microsoft also notes that all Automation Run As accounts that have been created using Azure Automation self-signed certificates between October 15, 2020, and October 15, 2021, are affected by the issue. Azure Migrate services and customers who deployed the preview version of VMware to Azure DR experience with Azure Site Recovery (ASR) might also be affected.

Thus, Azure AD customers should cycle through all Automation Account “Run as” certificates to make sure no credentials are exposed.

Related: Zero-Days Under Attack: Microsoft Plugs Exchange Server, Excel Holes

Related: Severe Vulnerabilities Could Expose Thousands of Azure Users to Attacks

Related: Microsoft Warns of Information Leak Flaw in Azure Container Instances

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Microsoft Informs Users of High-Severity Vulnerability in Azure AD
FBI Warns of Actively Exploited FatPipe Zero-Day Vulnerability
Cloud Data Protection Startup Laminar Closes $32M Funding Round
U.S., U.K. and Australia Warn of Iranian APTs Targeting Fortinet, Microsoft Exchange Flaws
Netgear Patches Code Execution Vulnerability Affecting Many Products

Tags:

NEWS & INDUSTRY Cloud Security Vulnerabilities