

CISA Ships 'Untitled Goose Tool' to Hunt for Microsoft Azure Cloud Infections

The U.S. government's cybersecurity agency CISA has jumped into the fray to help network defenders hunt for signs of compromise in Microsoft's Azure and M365 cloud deployments.

The agency rolled out a free hunt and incident response utility called Untitled Goose Tool that offers novel authentication and data gathering methods to manage a full investigation against enterprise deployments of Microsoft Azure, Azure Active Directory (AAD) and Microsoft 365 (M365).

In a note documenting the release, CISA said the Untitled Goose Tool can also gather additional telemetry from Microsoft Defender for Endpoint (MDE) and Defender for Internet of Things (IoT) (D4IoT).

The agency said Untitled Goose Tool was developed in tandem with researchers at Sandia National Laboratories to detect potentially malicious activity in Microsoft's growing cloud ecosystem.

Azure network defenders can use the tool to export and review sign-in audit logs and activity alerts from a range of Azure and Microsoft Defender environments to pinpoint signs of suspicious activity.

The tool can also be used to query, export, and investigate Azure Active Directory, M365, and Azure configurations.

According to CISA, defenders can ingest the JSON results from Untitled Goose Tool into a Security Information and Event

Management (SIEM) product, web browser, text editor, or a database.

“Network defenders attempting to interrogate a large M365 tenant via the UAL may find that manually gathering all events at once is not feasible,” CISA said, noting that its Untitled Goose Tool comes with “novel data gathering methods via bespoke mechanisms.”

The agency said cloud network administrators can use the tool to extract cloud artifacts from Microsoft’s AAD, Azure, and M365 environments without performing additional analytics.

According to CloudVulnDB, an open project tracking vulnerabilities affecting major cloud providers, there’s a long list of major security issues haunting Redmond’s flagship Azure and defenders have long complained about the lack of visibility into potential infections.

Microsoft has scrambled to mitigate several major security flaws affecting Azure, including code execution and cross-tenant data access issues. Some of the major issues include ChaosDB (exposed Azure customers’ database), SynLapse (impacted multiple Azure tenants), Azurescape (code execution and data access risks) and ExtraReplica (a collection of Azure bugs that exposed tenant databases).

Related: Microsoft Azure Vulnerability Allowed Code Execution

Related: Gem Security Gets \$11M Seed Funding for Cloud Incident Response Platform

Related: Critical Vulnerabilities in Azure PostgreSQL Exposed User Databases

Related: New Database Catalogs Cloud Vulnerabilities, Security Issues

<https://www.securityweek.com/cisa-ships-untitled-goose-tool-to-hunt-for-microsoft-azure-cloud-infections/>