Preliminary Post Incident Report
For
Microsoft 365

Report Date: October 1, 2020

Report By: ICC

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

Microsoft 365 Customer Ready Post Incident Report

Incident Information

Important Note	This is a preliminary Post Incident Report (PIR) that is being delivered prior to full incident resolution to provide early insight into details of the issue. The information in this PIR is preliminary and subject to change. A final PIR will be provided within five (5) business days from full event resolution and will supersede this document upon publication.
Incident ID	MO222965
Incident Title	Can't Access Microsoft 365 Services
Service(s) Impacted	Microsoft 365 Suite

User Impact

Users may have been unable to sign-in to Microsoft 365 services that leverage Azure Active Directory (Azure AD) authentication.

Affected Microsoft 365 services included the Microsoft admin center, Outlook, Outlook.com, Microsoft Teams, Teams Live events, SharePoint Online, Intune, Microsoft Forms, E911 services, Power Platform, and Dynamics 365 properties.

For E911 service impact: North America Teams users with Public Switched Telephone Network (PSTN) capabilities that were signed out at any point during the impact window may have been unable to sign back in and thus be unable to access the PSTN Dialpad. We've identified that 0.44% of E911 enabled Teams users could have been impacted; however, we have no record that any of these users attempted to make emergency calls during the period of impact.

Scope of Impact

This event may have impacted any users accessing Microsoft 365 services that leverage Azure AD authentication. Users who attempted to authenticate to services during the outage window may have received an error. Users who had authenticated prior to the impact start time were not likely to experience issues depending on the applications or services they were accessing.

We've identified that Azure AD authentication failures disproportionately affected users in North America and Asia Pacific due to the timing of the incident encompassing peak hours for both regions. The averages below represent availability by region and have been aggregated across our customer base.

- Europe: 81% success rate for the duration of the incident.
- Americas: 17% success rate for the duration of the incident, improving to 37% just before mitigation.
- Asia: 72% success rate in the first 120 minutes of the incident. As business-hours peak traffic started, availability dropped to 32% at its lowest.
- Australia: 37% success rate for the duration of the incident.

Incident Start Date and Time

Monday, September 28, 2020, at 9:25 PM UTC

Incident End Date and Time

Tuesday, September 29, 2020, at 12:23 AM UTC; though some customers may have experienced infrequent authentication failures which recovered by Tuesday, September 29, 2020, 2:25 AM UTC.

Root Cause

On September 28 at 9:25 PM UTC, a service update targeting an internal validation test ring was deployed, causing a crash upon startup in the Azure AD backend services. A latent code defect in the Azure AD backend service Safe Deployment Process (SDP) system caused this to deploy directly into our production environment, bypassing our normal validation process.

Azure AD is designed to be a geo-distributed service deployed in an active-active configuration with multiple partitions across multiple data centers around the world, built with isolation boundaries. Normally, changes initially target a validation ring that contains no customer data, followed by an inner ring that contains Microsoft only users, and lastly our production environment. These changes are deployed in phases across five rings over several days.

In this case, the SDP system failed to correctly target the validation test ring due to a latent defect that impacted the system's ability to interpret deployment metadata. Consequently, all rings were targeted concurrently. The incorrect deployment caused service availability to degrade.

Within minutes of impact, we took steps to revert the change using automated rollback systems which would normally have limited the duration and severity of impact. However, the latent defect in our SDP system had corrupted the deployment metadata, and we had to resort to manual rollback processes. This significantly extended the time to mitigate the issue.

Actions Taken (All times UTC)

Monday, September 28th, 2020

9:25 PM – Anomaly detection systems for authentications services, including Azure AD and Microsoft Teams, identified a potential issue. This coincided with social media reports of impact. We triggered a high-priority investigation.

9:28 PM – Our initial triage identified that one of a few Azure AD backend services was a potential cause of the event.

9:56 PM – We confirmed that multiple Microsoft 365 services were impacted by an issue with Azure AD. Initial triage from Microsoft Teams telemetry indicated a potential gateway issue.

10:02 PM – We identified the specific change to Azure AD that caused the event and began work to revert this update to mitigate impact.

10:21 PM – We began failing over Azure services to our backup authentication system.

10:45 PM – Our telemetry indicated that reverting the update did not restore service and we confirmed that the reversion failed. We began reviewing options for failing over SharePoint Online and Exchange Online services to the Azure AD backup authentication service, which also requires failing over authentication protocols from v2 to v1.

10:47 PM – We applied an alternate rollback mechanism to revert the root causing change, and recovery began.

11:28 PM – Service telemetry indicated that Microsoft Teams availability had increased to 60%, up from 26%. Additionally, we identified that a subset of backend components used to facilitate Azure authentication requests were still operating below acceptable performance thresholds. We began reconfiguring throttling parameters to

allow the backend components to recover. Furthermore, we performed traffic-management optimizations to assist with processing requests.
11:51 PM - The failover for SharePoint Online and Exchange Online to CSS authentication completed, and we began monitoring service telemetry for signs of recovery.
11:59 PM – We began manually reverting the service to the previous configuration.

Tuesday, September 29th, 2020
12:02 AM – SharePoint Online begins showing signs of service recovery.
12:14 AM – We triggered load-management processes to reduce traffic on a specific region for the DPX service, allowing the service to process a lower volume of requests and recover. Once the DPX service had recovered, we routed connections back to that region. Additionally, we performed a Microsoft Online Directory Services (MDOS) configuration change to provide further relief.
12:23 AM – Monitoring telemetry indicated that global Azure AD authentication systems reached acceptable performance thresholds; though, some regions may have seen residual impact for approximately two more hours.
12:31 AM – Service data showed that several Microsoft 365 services, including SPO and Microsoft Teams, started to see some recovery.
12:42 AM – The DPX service was performing within acceptable threshold and we continued to monitor the Microsoft 365 services.
12:50 AM – System telemetry indicated that Microsoft Teams had recovered.
1:27 AM – Telemetry indicated that most Azure authentication requests where being processed in a timely manner and impact had been mitigated for a large number of users. We identified that there was a small amount of residual impact in North America, Europe and Asia-Pacific regions.
2:25 AM UTC – Monitoring systems across Microsoft 365 services indicated the level of recovery had reached acceptable performance thresholds. We listed this as the end time in the admin center communications MO222695 and on status.office.com; although, a minority of users may have experienced residual impact.
2:30 AM – We confirmed that E911 services across the North America region were impacted by this issue. Additionally, we continued targeted restarts of Azure AD components to address residual user impact.
4:48 AM - After a period of extended monitoring, system telemetry showed that the service had remained healthy. We declared the incident fully resolved as of 2:25 AM.

Next Steps

Findings	Action	Completion Date
A code issue caused a portion of our infrastructure to experience delays processing authentication requests, which prevented users from being able to access multiple M365 services.	Fixed the latent code defect in the Azure AD backend SDP system.	Complete
Recovery was delayed due to rollback issues.	Fixed the existing rollback system to allow restoring the last known-good metadata to protect against corruption.	Complete
Manual rollback operations were sub-optimal.	Expand the scope and frequency of rollback operation drills.	Complete
Safe deployment process (SDP) did not provide adequate protection.	Apply additional protections to the Azure AD service backend SDP system to prevent the class of issues identified here.	Q4 2020
Azure AD backup authentication system is not integrated with all M365 services.	Expedite the rollout of Azure AD backup authentication system to all key services as a top priority to significantly reduce the impact of a similar type of issue in future.	Additional services in Q4 2020