

Important Update from Mimecast

 mimecast.com/blog/important-update-from-mimecast/



Microsoft recently informed us that a Mimecast-issued certificate provided to certain customers to authenticate Mimecast Sync and Recover, Continuity Monitor, and IEP products to Microsoft 365 Exchange Web Services has been compromised by a sophisticated threat actor.

Approximately 10 percent of our customers use this connection. Of those that do, there are indications that a low single digit number of our customers' M365 tenants were targeted. We have already contacted these customers to remediate the issue.

As a precaution, we are asking the subset of Mimecast customers using this certificate-based connection to immediately delete the existing connection within their M365 tenant and re-establish a new certificate-based connection using the new certificate we've made available. Taking this action does not impact inbound or outbound mail flow or associated security scanning.

The security of our customers is always our top priority. We have engaged a third-party forensics expert to assist in our investigation, and we will work closely with Microsoft and law enforcement as appropriate.

Forward-Looking Statements

This communication contains “forward-looking” statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995 and other federal securities laws, that are based on currently available information and our current beliefs, expectations and understanding. These forward-looking statements include statements regarding Mimecast’s current understanding of the cause and nature of the compromise of a certificate-based connection between Mimecast and Microsoft’s M365 Exchange Web Services, the scope and impact of the compromise, the number of targeted and impacted customers, the effectiveness of any current or future remediation efforts, the information provided to us by Microsoft and others in their investigations to date, the impact on our customers’ inbound or outbound mail flow and associated security scanning, and our ongoing investigation into this situation. Mimecast intends that all such forward-looking statements to be covered by the safe harbor provisions for forward-looking statements contained in Section 21E of the Securities Exchange Act of 1934, as amended, and the Private Securities Litigation Reform Act of 1995.

These statements are subject to future events, risks and uncertainties – many of which are beyond our control or are currently unknown to Mimecast. These risks and uncertainties include, but are not limited to, risks and uncertainties relating to the uncovering of new information in the course of our investigation related to the nature, cause and scope of the issue, the reputational, financial, legal and other risks related to potential adverse impacts to our customers and partners, and the other risks, uncertainties and factors detailed in Mimecast’s filings with the Securities and Exchange Commission. Mimecast is providing the information in this communication as of this date and assumes no obligations to update the information included in this communication or revise any forward-looking statements, whether as a result of new information, future events or otherwise.



[Up Next](#)

Email Security | Jan 21, 2021

Important Security Update