wandera

THREAT ADVISORY

Lycos Mail

SEVERITY	TYPE	IMPACT	TARGET	REPONSE
3/5	PII (PERSONALLY IDENTIFIABLE INFORMATION)	HIGH	WEBSITE	IMMEDIATE

SUMMARY

The threat research team at Wandera, with the help of MI:RIAM, has discovered a problematic data leak in a popular webmail service called Lycos Mail. This vulnerability puts individuals' usernames and passwords at risk of exposure. This is due to the transfer of said information unencrypted over-the-air during the login process.

Lycos Mail attracts over 650,000 visitors to its website every day, offering a no-fuss easy-to-use webmail service with 3GB of online storage. Lycos Mail also enables large file sharing as well as providing an intelligent spam filter.

The company is one of the original and most widely known Internet brands in the world, evolving from a search engine to a comprehensive digital media destination for consumers globally.

SECURITY IMPLICATIONS

The data leak has been identified by MI:RIAM as resulting from the transmission of sensitive data over the insecure and unencrypted HTTP channel.

This means the user's information travels over the internet in plaintext, making its exposure to third parties very likely. During the login process, where the leak has been detected, usernames and passwords are both made susceptible to attack.

Due to the nature of the information being exposed, hackers can easily gain access to users' Lycos e-mail accounts, where many keep the 'master keys' to their other private accounts. For example, if an individual has linked their e-mail account to Facebook or Twitter, a hacker can easily reset users' social media passwords simply by logging onto their e-mail accounts.

Additionally, because many people today utilize the same usernames and passwords for the majority of their accounts, by finding just one set of credentials, a hacker can usually infiltrate many of the individual's accounts. This undoubtedly increases the risk of identity or even monetary theft for Lycos Mail users.

RISK DETAILS

The PII (Personally Identifiable Information) exposed during the Lycos Mail login procedure include both username and password information.

LYCOS Mail

ABOUT THE LYCOS MAIL THREAT

What:
A website designed to provide users with access to e-mail services

Global impact:
Everyone using the mail.lycos.com website

Installations:
650,000 daily visits

Action required:
disable the HTTP protocol and adopt only HTTPs

REMEDIATION AND PREVENTION

Users should have an active mobile security service deployed on their device to monitor and block data leaks. This service should extend to browser activity as well as applications on the device.

Individuals should also avoid reusing sensitive information such as usernames and passwords for multiple applications and web services.

The developers of the Lycos webapp are advised to utilize SSL/TLS in order to protect the transmission of personally identifiable user information, session tokens, or other sensitive data to a backend API or web service.

REMEDIATION AND PREVENTION

We attempted to contact Lycos on three separate occasions over the course of 30 days to inform its security team of the data leak.

We received confirmations of receipt of our e-mails but no other response.