protiviti®
Face the Future with Confidence

Security Advisory – Outlook Web Access and Exchange Weaknesses Expose User Emails and Internal Networks

October 4,
2017

The majority of corporations leverage Microsoft Exchange as their primary email platform. In addition, many companies extend the use of corporate email to employees who work from home or while on the road. For these work-from-home employees, as well as "road warriors," to access their email, corporations often make their email system externally accessible via Outlook Web Access (OWA, Office365) or ActiveSync, which uses a feature called the Autodiscover service. This service minimizes user configuration and deployment steps by providing email clients access (Outlook) to Exchange features. For example, employees can open a web browser from their home computer or mobile phone and access their corporate email, or they can leverage the Autodiscover feature by using an email client.

What could be so wrong with extending this capability to employees? It does not grant them full internal network access, so what is the big deal with permitting this access?

Description of the Vulnerability

Weaknesses in Exchange and OWA email can expose user email accounts as well as enable a bad actor to gain remote access to the internal network and data. We have seen this as a likely attack vector in a recent publicized breach. In addition, a large portion of companies are vulnerable to this attack (which is relatively easy to execute) and should take immediate action to mitigate it.

Organizations are likely vulnerable if they do not use multi-factor authentication (MFA) on OWA (which is the common way it is implemented) and are running versions of Outlook and Exchange versions 2016 and older. OWA is susceptible to password-spraying ("brute force") attacks, where an attacker attempts to log in to the OWA portal by guessing the correct password for a valid user account. This is a very trivial attack and can be performed via automation scripts.

In addition, the Autodiscover service is susceptible to the same brute-force attacks. If you think limits on password-guessing attempts mitigate the risk from this attack, guess again. Lockouts can be evaded by limiting guessing to one or two commonly used passwords against many accounts. Also, passwords can be harvested from keystroke loggers and other malware on publicly accessible computers or other insecure systems that employees use to log on to OWA.

What's the risk if an attacker correctly guesses credentials or otherwise obtains a user's password? They have access only to that user's mailbox. It's not like attackers can leverage that access to further compromise the network. Or can they?

Scenario: An organization uses MFA on all remote access portals except OWA and extends the Autodiscover feature. The attacker performs a password-spraying attack against OWA and obtains one valid user account. The attacker not only has access to all the sensitive emails but can also look up the Exchange server configuration. The attacker then connects to the Exchange server via RPC/HTTP or MAPI/HTTP protocols discovered in the obtained configuration.

Using attacking tools, the attacker can create a custom Outlook rule or Outlook form to auto-execute a malicious file hosted on the internet. The attacker then sends an email to the compromised account, triggering the rule on the victim's Outlook application, which downloads and executes the malicious file on the user's workstation, creating a backdoor connection. The attacker can now leverage this connection to further compromise the internal corporate network.

What Should Organizations Do?

Organizations should immediately review their Exchange and email configuration to determine whether they are vulnerable to this issue. Many are likely vulnerable and therefore should investigate and implement controls to mitigate the associated risk. We have outlined several options to help address this problem. These options are intended as guidance only, as every organization may need to implement one or more of the following strategies depending on business constraints and technical limitations:

- Enforce MFA on OWA and Office365.
- Allow corporate email to be accessed only via an established virtual private network (VPN) connection, and do not allow OWA or Office365 web access.

- Research existing mobile device management (MDM) solutions and determine whether they can be leveraged to combat risk from Autodiscover being exposed to the internet and still allow mobile devices to receive email securely.
- Disable the Outlook client side rules from executing scripts or commands. (For more detailed guidance, see https://support.office.com/en-us/article/Custom-form-script-is-now-disabled-by-default-bd8ea308-733f-4728-bfcc-d7cce0120e94.)
- Enhance monitoring and alerting controls to detect malicious activity.

Lesson Learned – Make Sure You Can Detect as Well as Protect

Attacks like this one and recent breaches continue to reinforce the theme that it is not a matter of if you will be breached, but when. In addition to preventative measures such as those outlined above, organizations must work on maturing detective controls and response procedures. We continue to see breaches discovered long after the initial attack was successful. We also continue to see organizations mishandle the response activity, often making the damage from the breach worse.

Organizations must regularly assess and test the effectiveness of their detective processes. Activities that simulate common attack patterns should be carried out within organizations to determine whether their defenses can detect and respond accordingly. (We often refer to this type of test as purple team testing.) Organizations should utilize such testing or similar activity to regularly evaluate and refine their defensive posture to ensure that they can detect and respond accordingly.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®