НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Угроза раскрытия учетных данных пользователей при использовании службы Autodiscover в Microsoft Exchange Server

ALRT-20210924.1 | 24 сентября 2021 г.

Уровень угрозы: ВЫСОКИЙ

TLP: WHITE

Уязвимое программное обеспечение	Почтовые клиенты, поддерживающие работу с службой Autodiscover в Microsoft Exchange Server
Описание угрозы	Служба Autodiscover в Microsoft Exchange Server предназначена для упрощения процесса настройки почтовых клиентов и последующего подключения пользователей организации к функциям Exchange. Использование указанной выше службы позволяет пользователю получить доступ к функциям Exchange посредством ввода адреса электронной почты и пароля без необходимости дополнительных настроек. В рамках этого почтовый клиент попытается пройти аутентификацию по различным URL-адресам службы Autodiscover и получить необходимые настройки. При работе указанного механизма службе Autodiscover автоматически будут переданы учетные данные пользователя. URL-адреса формируются почтовым клиентом автоматически, исходя из введенного адреса электронной почты. Примером этого служит: Адрес электронной почты – user@example.ru URL-адреса автообнаружения: https://Autodiscover.example.ru/Autodiscover/Autodiscover.xml http://Autodiscover.example.ru/Autodiscover/Autodiscover.xml https://example.ru/Autodiscover/Autodiscover.xml http://example.ru/Autodiscover/Autodiscover.xml В случае если почтовый клиент не смог пройти аутентификацию по таким URL-адресам, он выполнит генерацию дополнительного адреса. Таким адресом будет доменное имя autodiscover.[TLD], где [TLD] является производным от адреса электронной почты пользователя. В вышеуказанном случае сгенерированный URL-адрес будет выглядеть следующим образом: http://Autodiscover.ru/Autodiscover/Autodiscover.xml Это создает предпосылки к тому, что почтовые клиенты могут осуществить попытку проверки подлинности клиента на стороннем ресурсе autodiscover.ru. Таким образом владелец доменного имени получит возможность собирать любые отправленные ему учетные данные пользователей.

	Кроме этого, в открытых источниках имеются сведения о наличии средств, которые позволяют обойти механизмы NTLM и Oauth и понизить метод аутентификации до уровня простой проверки подлинности пользователя. В результате этого учетные данные пользователя будут переданы в открытом виде.
Рекомендации по нейтрализации угрозы	Для организаций, использующих Microsoft Exchange, необходимо заблокировать доменное имя Autodiscover.[TLD] на брандмауэре или DNS-сервере, чтобы устройства не могли подключиться к нему. Отключить для пользователей возможность базовой аутентификации в почтовых клиентах, так как при ее использовании учетные данные передаются в открытом виде.
Ссылки на источники	https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-autodiscover-bugs-leak-100k-windows-credentials/