НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Угроза безопасности информации при эксплуатации уязвимости в Microsoft Exchange Server

ALRT-20210903.1 | 3 сентября 2021 г.

Уровень угрозы: ВЫСОКИЙ

TLP: WHITE

Уязвимое программное обеспечение	Microsoft Exchange Server 2013, 2016, 2019	
Актуальность угрозы	По настоящее время	
Описание угрозы	Уязвимость позволяет удаленному злоумышленнику получить доступ к конфиденциальной информации в целевой системе посредством отправки специально сформированного вредоносного запроса к веб-сервису Exchange Control Panel (ECP). Уязвимость обусловлена небезопасной процедурой аутентификации на почтовом сервере через веб-службы Microsoft Exchange (Outlook Web Access, ECP). Указанная уязвимость актуальна только в случае установленного модуля ECP. Злоумышленник должен отправить запрос на авторизацию со специально сформированным файлом cookie и именем SecurityToken, данный запрос на аутентификацию будет делегирован от веб-сервисов к серверной части. Если со стороны серверной части не происходит загрузка модуля DelegatedAuthModule, то некоторые запросы будут пропущены без аутентификации. С подгруженным модулем DelegatedAuthModule на данный запрос от серверной части Microsoft Exchange вернется ответ с ошибкой HTTP 500, содержащий canary-токен ECP. Используя полученный canary-токен, злоумышленник может обойти процесс аутентификации и изменить некоторые параметры в конфигурации Microsoft Exchange Server, например, настроить правило для конкретного почтового адреса, осуществляющее пересылку всех входящих почтовых сообщений на контролируемый злоумышленником почтовый адрес.	
CVE-2021-33766	Наименование уязвимого продукта	Microsoft Exchange Server
	Версии уязвимого продукта	Microsoft Exchange Server 2019 до Cumulative Update 8 Microsoft Exchange Server 2019 до Cumulative Update 9 Microsoft Exchange Server 2016 до Cumulative Update 19 Microsoft Exchange Server 2016 до Cumulative Update 20 Microsoft Exchange Server 2013 до Cumulative Update 23
	Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
	Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
	Вектор атаки	Сетевой
	Взаимодействие с пользователем	Нет
	Последствия эксплуатации уязвимости	Раскрытие информации
	Средства устранения уязвимости	Официальное решение

	Дата выявления	14.07.2021
	Дата обновления	30.08.2021
	Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Рекомендации по нейтрализации угрозы	Обновить программное обеспечение	
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2021-33766 https://www.zerodayinitiative.com/blog/2021/8/30/proxytoken-an-authentication-bypass-in-microsoft-exchange-server https://www.zerodayinitiative.com/advisories/ZDI-21-798/ https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-33766	