Кібератака на державні організації України з використанням експлойту для XSS вразливості в Zimbra Collaboration Suite (CVE-2018-6882) (CERT-UA#4461)

Загальна інформація:

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA від суб'єкту координації отримано електронний лист з темою "Volodymyr Zelenskyy presented the Golden Star Orders to servicemen of the Armed Forces of Ukraine and members of the families of the fallen Heroes of Ukraine" та декількома графічними зображеннями.

За результатами дослідження з'ясовано, що заголовок листа "Content-Location" містить JavaScript-код, виконання якого призведе до завантаження і виконання іншого JavaScript-коду, призначенням якого є додавання до конфігурації облікового запису електронної пошти жертви сторонньої електронної адреси з метою подальшого пересилання на неї електронних листів користувача.

Технічна можливість реалізації описаної загрози класифікована за ідентифікатором CVE-2018-6882 як XSS (Cross-Site Scripting) вразливість в Zimbra Collaboration Suite (< 8.7 Patch 1, 8.8.x < 8.8.7).

Виявлена активність, зважаючи на тему, вміст, додатки до листа, а також отримувачів, носить цільовий характер та відстежуватиметься за ідентифікатором UAC-0097.

Індикатори компрометації:

Файли:

```
ddeab2d94128abbf9b4bf8ade4f9919e
ad75a9a8eb1210d04873c151ada56520d582cc1012a50895d6c06bb60160d6b8
junit.js
```

Мережеві:

```
joey@kmtacn[.]com (X-FE-Envelope-From)
211.234.110[.]194 (X-FE-Last-Public-Client-IP)
hxxps://cdn.jsdelivr[.]net/gh/sukaut/beta@main/junit.js
repo.ma@hotmail[.]com (адреса електронної пошти для ексфільтрації)
nov.td@yandex[.]ru (пов'язана адреса електронної пошти)
hxxps://github[.]com/sukaut (відповідний репозиторій в GitHub)
```

Рекомендації:

1. Забезпечити своєчасне оновлення програмного забезпечення Zimbra.

2. Забезпечити безпечне налаштування програмного забезпечення Zimbra відповідно до кращих практик (hxxps://wiki.zimbra[.]com/wiki/SecureConfiguration).

3. Вжити заходів з перевірки наявності налаштувань, що стосуються фільтрів та/або пересилання електронних листів (використовується як засіб ексфільтрації даних).

Графічні зображення: