*Ria Siti Juairiah, 09011281520128*

1. **Tentang CVE**

Dalam keamanan informasi, **Vulnerability** dan **Exposure** adalahcelah dalam sebuah software yang digunakan oleh peretas untuk masuk ke sebuah sistem informasi dan melakukan aktivitas yang tidak sah dengan menyamar sebagai pengguna yang berwenang.

Tujuan utama CVE adalah berbagi data tentang vulnerabiities dan exposure yang sudah pernah terjadi diberbagai database dan menjelaskan apa dampaknya. Sehingga CVE membantu vendor keamanan komputer untuk mengidentifikasikan lebih cepat vulnerabilities dan exposures.

1. **Jenis Penyerangan**

Salah satu CVE yang terdaftar adalah CVE-2014-0521 dengan deskripsi *Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X do not properly implement JavaScript APIs, which allows remote attackers to obtain sensitive information via a crafted PDF document*. CVE-2014-0521 memungkinkan peretas untuk mendapatkan informasi yang sensitif via PDF buatan. Penyerangan ini dapat dilakukan pada komputer yang menggunakan Adobe Reader dan Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X.

Secara umum penyerangan ini dapat menyebabkan penyerang mendapatkan informasi sensitif berupa alamat akun dan password dan juga menyebabkan penyerang dapat menguasai sistem komputer yang digunakan oleh korban. Dari penguasaan sistem komputer ini, penyerang dapat mengendalikan, melihat data, menghapus atau membuat data didalam komputer tersebut. Penyerangan jenis ini termasuk pemalsuan email, pencantuman PDF yang sudah memiliki code tertentu, dan pemalsuan website.

1. **How To Attack**
2. **Tujuan hanya untuk mendapatkan informasi akun**
3. Pishier (penyerang) akan mencantumkan lampiran PDF jebakan didalam pesan email. Email ini seolah-olah berasal dari lembaga atau perusahaan resmi.
4. Ketika lampiran dibuka, akan muncul PDF yang berbentuk seperti pesan error. Pesan ini berisi perintah untuk membuka dokumen itu dengan Microsoft Excel. Kenyataannya, file ini akan langsung terhubung dengan website.
5. Ketika user memilih link persetujuan untuk membuka file melalui Microsoft Excel, maka otomatis akan masuk kesebuah website palsu. Di website ini penyerangan jenis social engineering berlanjut dengan sebuah pesan bahwa dokumen ini sangat penting sehingga dilindungi dan user harus sign in ke email terlebih dahulu untuk membuka proteksi itu.

Penyerangan ini dapat mengakibatkan penyerang mengetahui nama akun dan password email user. Penyerang dapat menggunakan semua konten yang terikat dengan akun tersebut. Bergantung pada hak istimewa yang terkait dengan pengguna, penyerang kemudian dapat menginstal program; melihat, mengubah, atau menghapus data; atau buat akun baru dengan hak pengguna penuh. Ini akan sangat berpengaruh untuk pengguna yang menggunakan akun emailnya di konten yang snagat penting.

1. **Tujuan untuk menguasai sistem komputer korban**
2. Pishier (penyerang) akan mencantumkan lampiran PDF jebakan didalam pesan email. Email ini seolah-olah berasal dari lembaga atau perusahaan resmi. PDF ini dibuat dengan code atau command line tertentu.
3. Ketika lampiran dibuka melalui Adobe Reader, code atau command yang tertulis di PDF akan otomatis aktif. Beberapa jenis command line tertentu dapat mengakibatkan penyerang di izinkan untuk mengakses bebas informasi lokal komputer korban. Command line juga bisa mengunduh malware dari internet sehingga komputer terinfeksi oleh malware tersebut.

File PDF yang sudah mengakali URI akan mengeksploit kelemahannya dan akan mengakses *cmd.exe* dan menjalankan sebuah rantai instruksi windows untuk melakukan aksi berikut:

* Menghilangkan firewall windows
* Menciptakan file temporer “I” dengan ftp commands.
* File “I” tersebut mengandung informasi untuk mendownload file berbahaya “system.com”,
* Menggunakan [ftp.exe](ftp://ftp.exe) dan ftp command file “I” untuk men-download malware
* Mengeksekusi malware yang sudah terdownload.

**REFERENSI**

Anonymous. “Adobe Security Bulletin”. Diakses pada 18 Februari 2018 <https://helpx.adobe.com/security/products/reader/apsb14-15.html>

Anonymous. “CVE-2014-0521”. Diakses pada 18 Februari 2018 <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0521>

Anonymous. “Common Vulnerabilities and Exposure”.Diakses pada 19 Februari 2018 dari <https://www.techopedia.com/definition/16075/common-vulnerabilities-and-exposures-cve>

Landau, Ted. “Bug and Fix : Adobe Reader Phising Scam”. Diakses pada 19 Februari 2018 dari <https://www.pcworld.com/article/188234/article.html>

Teppalavalasa, Satyendra. “Serangan Terhadap Portable Document Format (PDF). Diakses pada 19 Februari 2018 dari <https://lightoftheday.wordpress.com/2010/12/23/serangan-terhadap-portable-document-format-pdf/>

Webmaster. “Pishing Attack by Social Engineering Technologies via PDF”. Diakses pada 18 Februari 2018 dari <http://www.computergk.com/email-phishing-attack-by-social-engg-tech-via-pdf-attachments/>