PEMOGRAMAN MANAJEMEN KEAMANAN INFORMASI
"Scanning Network dan Scanning Sistem Pada Web deviantart.com dan wonogirikab.go.id "

Dibuat oleh :

M.Rahmat Romadhan (09031281520095)

JURUSAN SISTEM INFORMASI

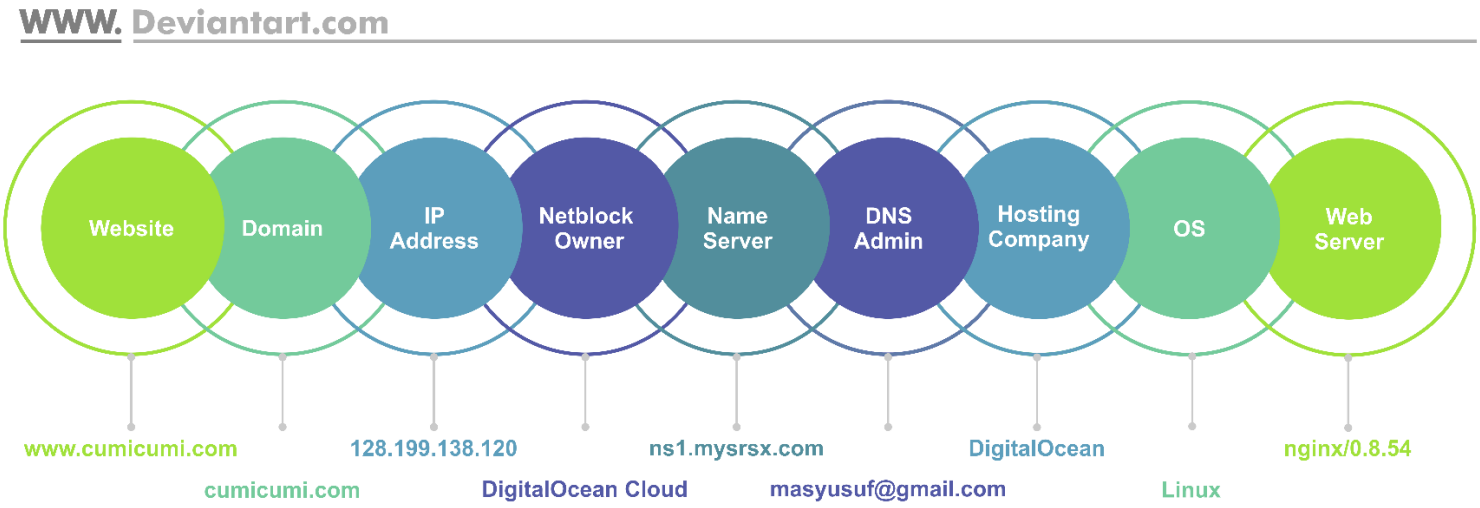
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

PALEMBANG

2018

Hasil site report dari www.deviantart.com menggunakan netcraft



Kelemahan web server dan OS dari www.deviantart.com menggunakan CVE

Di PHP melalui 5.6.33, 7.0.x sebelum 7.0.28, 7.1.x sampai 7.1.14, dan 7.2.x sampai 7.2.2, ada buffer berbasis stack yang dibaca sementara mengurai respons HTTP di php_stream_url_wrap_http_ex berfungsi di ext / standard / http_fopen_wrapper.c. Ini kemudian menghasilkan penyalinan string besar.

Stump berbasis Buffer Overflow di httpd pada perangkat Tenda AC9 V15.03.05.14_EN memungkinkan penyerang jarak jauh menyebabkan penolakan layanan atau mungkin memiliki dampak lain yang tidak ditentukan.

Di /usr/local/etc/config/addons/mh/loopupd.sh pada perangkat eQ-3 AG HomeMatic CCU2 2.29.22, paket pembaruan perangkat lunak didownload melalui protokol HTTP, yang tidak menyediakan perlindungan kriptografi dari konten yang didownload . Penyerang dengan posisi jaringan istimewa (yang dapat diperoleh melalui spoofing DNS www.meine-homematic.de atau pendekatan lainnya) dapat memanfaatkan masalah ini untuk memberikan pembaruan firmware jahat yang sewenang-wenang ke CCU2. Hal ini bisa mengakibatkan kompromi sistem penuh.

Pemasang FSX / P3Dv4 2.0.1.231 untuk Flight Sim Labs A320-X mengirimkan kredensial akun Google pengguna ke http://installLog.flightsimlabs.com/LogHandler3.ashx jika nomor seri bajakan telah dimasukkan, yang memungkinkan penyerang jarak jauh memperoleh informasi sensitif, misalnya dengan mengendus jaringan untuk lalu lintas HTTP cleartext. Perilaku ini telah dihapus di 2.0.1.232.

Hasil site report dari www.wonogirikab.go.id menggunakan netcraft

Kelemahan web server dan OS dari www.wonogirikab.go.id menggunakan CVE

- Kebocoran memori dalam fungsi zlib_stateful_finish di kripto / comp / c_zlib.c di OpenSSL 0.9.8l dan sebelumnya dan 1.0.0 Beta sampai Beta 4 memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (konsumsi memori) melalui vektor yang memicu panggilan yang salah ke Fungsi CRYPTO_cleanup_all_ex_data, seperti yang ditunjukkan dengan penggunaan SSLv3 dan PHP dengan Apache HTTP Server, sebuah isu terkait dengan CVE-2008-1678.
- Layanan pengarsipan proses ODE sangat masuk akal untuk menyebarkan pesan dengan nama palsu. Menggunakan jalur untuk nama itu memungkinkan traversal direktori, sehingga berpotensi menulis file di bawah lokasi yang tidak diinginkan, Timpa file yang ada atau penghapusannya. Masalah ini dibahas di Apache ODE 1.3.3 yang dirilis pada tahun 2009, namun nama yang salah CVE-2008-2370 digunakan pada penasehat karena kesalahan.
- Di Apache jUDDI 3.2 sampai 3.3.4, jika menggunakan kelas WADL2Java atau WSDL2Java, yang mengurai dokumen XML lokal atau jauh dan kemudian memediasi struktur data ke dalam struktur data UDDI, ada sedikit perlindungan yang hadir terhadap perluasan entitas dan jenis serangan DTD. Mitigasi adalah menggunakan 3.3.5.
- Batasan keamanan yang ditentukan oleh anotasi Servlets di Apache Tomcat 9.0.0.M1 sampai 9.0.4, 8.5.0 sampai 8.5.27, 8.0.0.RC1 sampai 8.0.49 dan 7.0.0 sampai 7.0.84 hanya diterapkan sekali Servlet telah dimuat. Karena kendala keamanan yang didefinisikan dengan cara ini berlaku untuk pola URL dan URL mana pun di bawah titik itu, mungkin - tergantung pada pesanan Servlets dimuat - untuk beberapa batasan keamanan yang tidak diterapkan. Ini bisa saja membuka sumber daya bagi pengguna yang tidak berwenang mengaksesnya.