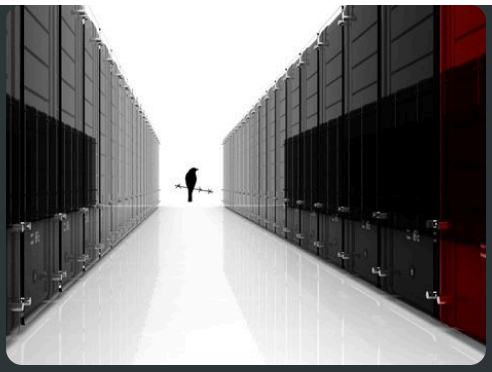
advisory

ØDAY ADVISORY AUTHENTICATION CVE CYBER DJANGO EXPLOIT HACKING LOGPOINT METASPLOIT MIDDLEWARE PRODUCT SECURITY VULNERABILITY

OCT 8, 2017

One ring to rule them all - Same RCE on multiple Trend Micro products

Framework's security has been a known topic for security folks. In fact, we already seen a real impact of single vulnerability within a framework on Apache Struts case. If we consider this risk from the point of products vendor, we could see very similar case. In this article, I will show you how we get RCE on different Trend Micro products because of same codebase used by across the different products.
(more…)



SEP 19, 2017

Advisory | DenyAll Web Application Firewall Unauthenticated Remote Code Execution (CVE-2017-14706)

DenyAll Web Application Firewall is the foundation for next generation application security products. It combines ease of configuration - with its workflow engine and management APIs - with a proven ability to secure web applications. It embeds negative and positive security, in-context, user behavior analysis, and soon-to-be added rWeb advanced security engines, to efficiently protect your web applications while minimizing false positives.
(more…)

SEP 12, 2017

Advisory | osTicket v1.10 Unauthenticated SQL Injection (CVE-2017-14396)

osTicket is a widely-used and trusted open source support ticket system. It seamlessly routes inquiries created via email, web-forms and phone calls into a simple, easy-to-use, multi-user, web-based customer support platform. osTicket comes packed with more features and tools than most of the expensive (and complex) support ticket systems on the market.

(more…)

AUG 6, 2017

Exploiting Second Order SQLi Flaws by using Burp & Custom Sqlmap Tamper

Web applications evolved in the last century from simple scripts to single page applications. Such complex web applications are prone to different types of security vulnerabilities. One type of vulnerability, named as secondorder, occurs when an attack payload is first stored by the application on the web server and then later on used in a security-critical operation.
(more…)

JUN 10, 2017

Unexpected Journey #5 - From weak password to RCE on Symantec Messaging Gateway (CVE-2017-6326)

If you are following our blog, you must familiar with Unexpected Journey article series. In this article, I will share our latest real-life pentest experience as well

as the technical details of our brand new ~~0day~~ that helps us to execute operating system commands on Symantec Messaging Gateway.
(more…)

MAY 17, 2017

Advisory | Cryptolog Unauthenticated Remote Code Execution

CRYPTOLOG is a log manager that collects, normalizes, and categorizes massive logs generated across your network and turn it into valuable information on an intuitive interface where advance search, analysis and correlation monitoring becomes easier and more efficient.
(more…)

MAR 17, 2017

Unexpected Journey #4 - Escaping from Restricted Shell and Gaining Root Access to SolarWinds Log & Event Manager (SIEM) Product

By time goes, I've found myself more focusing on SIEM product during penetration test. This is the fourth article of my article series called as "Unexpected Journey" which

all of them focused on different SIEM products. In this article, I will share the details how I've got root access to the SolarWinds Log & Event Management product. (more…)

MAR 7, 2017

Unexpected Journey #3 - Visiting Another SIEM and Uncovering Pre-auth Privileged Remote Code Execution

This is the third part of our article series that intended to share my real-life penetration testing experience.In this article, I will share a whole process of how we managed to find a -0day- pre-auth RCE vulnerability on another SIEM product. (more…)

FEB 7, 2017

Advisory | CVE-2017-6398 Trend Micro InterScan Messaging Security (Virtual Appliance) Remote Code Execution

In this article, we will show details and metasploit module for vulnerability that affects Trend Micro's IMSVA solution.

(more…)

JAN 7, 2017

Unexpected Journey into the AlienVault OSSIM/USM During Engagement

Being a penetration tester makes us feel like a group of traveler. Discovering the internal world of the institution during engagement gives us the opportunity to make unexpected journeys. In this article, I will share a details of how we got an access to the heart of the company.
(more…)