coresecurity
by HelpSystems

DATASHEET *(Cybersecurity)*

ExCraft Exploits Designed for Core Impact

Exploitation packages designed for Core Impact and maintained by security experts from ExCraft Labs

In order to provide Core Impact users with the most comprehensive and trustworthy exploit library on the market, Core Security partners with ExCraft Labs, an expert cybersecurity research group, to provide additional enhancements. Since 2013, ExCraft Labs has been researching vulnerabilities and writing exploits designed for the Core Impact pen testing framework. These regularly updated and validated exploit packs are available for purchase directly through Core Security, a HelpSystems Company.

Exploits are a critical component in pen testing. Threat actors use exploits to take advantage of flaws or weaknesses in an application or software, pen testers must also utilize them in order to authentically demonstrate how much risk these weaknesses may pose to an organization.

However, Core Security uses a thorough vetting process and takes care to never allow the purchase of Core Impact and its corresponding exploit library--including these additional exploit packs--by any organization that intends to use them for malicious purposes.

ExCraft SCADA Exploit Pack: Standard and Professional

Supervisory control and data acquisition (SCADA) and other industrial control systems (ICS) have become essential to industrial processes like manufacturing, production, development, and fabrication.They monitor and control the equipment in these processes, centralizing operations. Since they are so critical, these systems have caught the eye of threat actors. Gaining access and control of a SCADA system provides them with the keys to the kingdom, and can completely cripple operations. This has made pen testing SCADA and ICS a high priority for any organization that relies on them to maintain productivity.

SCADA and ICS focused exploitation packages designed to greatly increase SCADA pen testing capabilities with Core Impact. Both standard and professional packages are available.

Standard	Professional
Hundreds of modules for public and commercial vulnerabilities	Includes all standard pack modules and 0Days
Basic level ICS pen testing	0 Days in the latest versions (tested within a month after latest version release)
2-5 new exploits included in every monthly update	5-7 high risk scored vulnerabilities and exploits in every month update
Basic level exploits: DoS, SQLi, triggers, PoC	Professional level exploits: tricky SQLi, RCE, complex BOF, Trojans, and more.

ExCraft Medical Exploit Pack

Healthcare technology is a broad field that has, and will continue to experience massive growth over the years. As medical information continues its shift from paper to digital, threat actors have zeroed in on the industry as a prime target for accessing sensitive information. Additionally, organizations in this industry must remain in compliance with the Health Insurance Portability and Accountability Act (HIPAA). Pen testing is a particularly critical tool for organizations assessing their security infrastructure.

The ExCraft Medical Pack is designed for testing software and hardware related to human and animals health, including Health Information Management Systems, electronic medical charts, dental accounting software, and more. This pack is ideally suited for clinical systems penetration testing. This pack is updated monthly with 1-2 new exploits or tools in every release.

ExCraft IoT Exploit Pack

IoT devices have added significant benefits to productivity, but they have also significantly broadened the security perimeter, increasing any organization's attack surface. Connecting IoT devices to an organization's network is particularly risky they often lack traditional preventative layers like antivirus, making them ideal entry points. Uncovering any potential vulnerabilities in these devices through pen testing is a key way to ensure these devices are as secure as possible.

The ExCraft IoT Pack is designed for vulnerabilities in IOT devices or related software. These exploits can be useful in virtually every penetration test, covering network cameras, TV sets, IoT, routers, and DVRs. It is updated monthly and includes 2-6 new exploits or tools in every release.