ESSENTIAL

CAPABILITY SUBSCRIPTION

EXODUS INTELLIGENCE

This subscription provides the core tools that belong in the toolbox of every group conducting offensive security engagements. These groups include law enforcement, government agencies, and commercial penetration testers. The Essential Capability Subscription provides these groups with production grade exploits that provide access to software with high market share. Exodus has staffed this subscription with some of the top exploit writers and researchers in the industry, including many past pwn2own and PWNIE winners.

This offering is for non-exclusive rights to all of Exodus' exploit research for the extent of the subscription terms. Below are some of the capabilities that are maintained in the Essential Capability Subscription.

- Browser Chain (Microsoft Internet Explorer or Edge, Mozilla Firefox, Safari, or Chrome)
- LPE – default local privilege escalation in major OS (Windows, Linux, or Mac)
- Adobe Reader/Acrobat, Microsoft Office, Flash, or equivalent client-side software
- Virtual Machine Escape (VMWare, Virtual Box, Hyper-V, Docker, Kubernetes)
- Enterprise Router, Switches, Modems
- Market leading Firewall solutions
- Cyber Security Products – Antivirus, end point detection, DLP
- System Infrastructure (apache/active dir/etc)

We guarantee a minimum of 4 capabilities from the above list will be maintained throughout the year. If one is patched, we guarantee a replacement within 3 months. All exploits are tested continuously in our QA environment for reliability, code updates, and product coverage. The following capabilities were available to subscribers of the Essential Capability Subscription in 2020:

- Windows 10 Local Privilege Escalation (1803+)
- MacOS Safari Local Privilege Escalation
- MacOS Local Privilege Escalation
- MacOS/iOS Webkit Randomization Mitigation Bypass
- MacOS/iOS Safari Remote Code Execution
- Oracle Virtualbox Guest-to-Host Escape
- Windows DWM Local Privilege Escalation
- Windows 7 Local Privilege Escalation
- Windows UAC Bypass
- Microsoft Edge Remote Code Execution
- Microsoft Edge Sandbox Escape
- MacOS Safari Sandbox Escape
- Windows Defender SmartScreen Bypass
- Mozilla Firefox JavaScript Privilege Escalation
- Foxit Reader/PhantomPDF Remote Code Execution

THE RESEARCH

WHAT OUR CUSTOMERS RECEIVE

ENHANCE NETWORK DEFENSE WITH EXODUS' ENRICHED VULNERABILITY INTELLIGENCE FOR HIGH-PROFILE VENDORS

COMMERCIAL

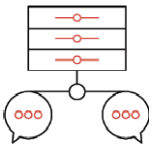
- Microsoft
- Adobe
- EMC
- Novell
- IBM, and others

INDUSTRIAL CONTROL SYSTEMS

- Siemens
- General Electric
- Rockwell Automation, and others

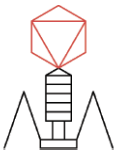
Exodus offers highly enriched, valuable intelligence that enables you to test and optimize your defenses with precision. Every vulnerability is analyzed and well documented. Our Vulnerability Research Packages include:

VULNERABILITY INTELLIGENCE REPORT
Understand all aspects of the vulnerability



NETWORK PACKET CAPTURE
See both malicious and benign traffic

XML | RESTful API | STIX/TAXII
Integrate defenses into third-party SIEM or other defensive products



METASPLOIT MODULE
Test your defenses with a working exploit or proof-of-concept

VULNERABILITY INTELLIGENCE REPORT

The report is 15 to 30 pages covering all aspects of the vulnerability, including:

- Affected products, versions, supported architectures, and hashes of binary files
- Target market share, common usage, and typical deployment configurations
- Technical information on the vulnerable components and enumeration of attack vectors
- Disassembly and/or source code
- Walkthroughs showing the flaws in the code
- Detailed information on attack vectors and corresponding malicious network traffic
- Guidance on how to detect an attack in progress, as well as artifacts left behind in the case of a successful compromise
- An explanation of the complete exploitation process, including bypassing mitigations
- Insight into the requirements, reliability, difficulty, and likelihood of an attacker successfully exploiting the issue
- Guidance on reducing or eliminating susceptibility to the flaw in place of an official patch from the affected vendor

CALL US FOR A FREE CONSULTATION
512-888-9770 | INFO@EXODUSINTEL.COM