OFFERINGS

EXODUS INTELLIGENCE

Exodus Intelligence provides clients with exclusive vulnerability intelligence and proof of concepts affecting widely used and relied upon software. This information is made available to clients by means of an annual subscription to one of Exodus' various intelligence feeds, as detailed below.

ZERO-DAY SUBSCRIPTION

Customers responsible for maintaining awareness regarding unknown threats to their enterprise networks are able to subscribe to the Exodus Intelligence enterprise zero-day feed (Enterprise Zero-Day Feed). This offering gives the customer access to an average of 50 unique zero-day reports and corresponding trigger (proof of concept) for vulnerabilities discovered by the Exodus team throughout a 12 month period. Typically, flaws included in such a subscription affect high-profile vendors such as Microsoft, Adobe, EMC, Novell, IBM, and others.

Included with a subscription to this offering, customers are kept apprised of exclusive vulnerabilities and threats in Industrial Control Systems. Typically, the flaws included affect high-profile vendors such as Siemens, General Electric, Rockwell Automation, and others. Vulnerabilities included in this offering are not reported to the affected vendors and as such the information is available exclusively to Exodus customers.

N-DAY SUBSCRIPTION

In addition to researching exclusive zero-day vulnerabilities, Exodus Intelligence also offers a few tiers of a N-day feed comprised of threats that have been publicly disclosed by outside organizations or the vendors themselves. These vulnerabilities are investigated, analyzed and documented for distribution to customers. Subscribers of this offering gain access to an arsenal of proof-of-concepts and corresponding documentation enabling them to ensure their defensive measures have been implemented properly.

THE RESEARCH

WHAT OUR CUSTOMERS RECEIVE

EXODUS INTELLIGENCE

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

COMMERCIAL

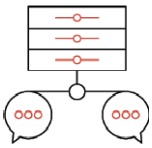
- Microsoft
- Adobe
- EMC
- Novell
- IBM, and others

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 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