N-DAY
VULNERABILITY SUBSCRIPTION

EXODUS INTELLIGENCE

DON'T LEAVE YOUR CYBERSECURITY TO VENDOR PATCHES

Exodus Intelligence's N-Day Vulnerability subscription provides customers with intelligence about critically exploitable, publicly disclosed vulnerabilities on widely used software and hardware. Every vulnerability is analyzed, documented and enriched with high-impact intelligence derived by some of the best reverse engineers in the world. At times, Vendor patches fail to properly secure the underlying vulnerability. Enhance your patch management efforts by subscribing to Exodus' arsenal of more than 1000 vulnerability intelligence packages to ensure defensive measures are properly implemented. Exodus enables you to focus resources on detecting and mitigating the most serious threats to your enterprise for less than the cost of a single cybersecurity engineer.

ADVANCED THREAT DETECTION

We develop proof of concepts for known vulnerabilities in order to help customers detect and prioritize the most serious threats.

ACTIONABLE MITIGATION GUIDANCE

Our elite reverse engineers examine the root cause of the vulnerabilities in order to demonstrate the impact of the threat and help customers harden defenses with actionable mitigation guidance.

PATCH ANALYSIS

Failed patches leave organizations at risk. Exodus examines publicly disclosed, critically exploitable vulnerabilities to verify patch effectiveness and present enriched intelligence about affected software and systems.

THE VAULT

Customers access the entire repository of our vulnerability research held in our Vault. The enriched vulnerability intelligence enables customers with high efficacy decision ready information to implement meaningful risk management actions.

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

THE RESEARCH

WHAT OUR CUSTOMERS RECEIVE

EXODUS INTELLIGENCE

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

COMMERCIAL

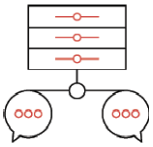
- Microsoft
- Adobe
- EMC
- Novell
- IBM, and others

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 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