PREDICTING EXPLOITABILITY

YES/NO FORECAST FOR VULNERABILITY MANAGEMENT

NorthStar PREDICTION ENGINE

EASY ANSWERS TO HARD QUESTIONS

Is your vulnerability management program able to clearly delineate between vulnerabilities that are unexploited versus ones that are either currently being actively exploited in the wild or are predicted to be exploited in the wild?

NorthStar is the ultimate vulnerability prioritization and prediction engine.

In addition to automatically identifying vulnerabilities currently being exploited in the wild, NorthStar's vulnerability prediction engine accurately identified over 45% of the vulnerabilities that would be exploited in the wild at some point in the future, providing an average notice of around 280 days in advance.

45%
OF THE CVES ARE VALIDATED AS EXPLOITED IN THE WILD

280
DAYS ADVANCE NOTICE

97%
REDUCTION IN THE NUMBER OF CVES TO FOCUS ON

HOW IT WORKS

Prediction begins with the collection of surveillance data that captures the footprint or breadcrumbs left behind on-line by attackers seeking to develop, deploy, and monetize exploits that are capable of leveraging an existing vulnerability. The appearance of these events and activities have proven reliable in determining the immediate risk posed by each vulnerability.

NorthStar's vulnerability prediction engine is a **yes/no categorical prediction**. This provides a definitive assessment on whether a CVE will eventually be exploited in the wild. Each prediction comes with a timestamp representing when the prediction was first made based on all available data at the time.

WHY NORTHSTAR?

Sometimes in life, it's the small decisions that create the biggest impact. Just because a CVE has an exploit, it does not mean it has ever been used in the wild. Don't get stuck relying on an exploit probability score that leaves you questioning where to draw the line.

NorthStar predicts the **application of exploit to a CVE** and our results are validated by industry leading threat intelligence feeds.

CVE	DESCRIPTION	CVE PUBLISH DATE	NORTHSTAR PREDICTION DATE	EXPLOITED IN THE WILD	CVSS CRITICALITY SCORE
CVE-2019-11510	In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability.	**2019-05-08**	**2019-09-01**	**2020-09-17**	**10.0**
CVE-2019-19781	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.	**2019-12-27**	**2020-01-15**	**2020-03-25**	**9.8**

NorthStar leverages active attacker tool imagery and all available vulnerability data to predict if an exploit will be created and used in the wild for a particular vulnerability. In the examples above, NorthStar predicted CVE-2019-11510 **386 days in advance** and CVE-2020-15505 **47 days in advance** of either being exploited in the wild.

Confidently anticipate future exploits with a definite **YES** from NorthStar Prediction Engine.

516 N. Ogden Ave Suite 115
Chicago, IL 60642

Give us a call
312.421.3270

Send us an email:
connect@northstar.io

For more info, visit us at:
www.northstar.io

NorthStar