

# ZERO DAY INITIATIVE

## PROMOTING COORDINATED VULNERABILITY DISCLOSURE

The Zero Day Initiative™ (ZDI) was founded in 2005 to encourage the coordinated reporting of zero-day vulnerabilities to affected vendors by financially rewarding researchers through incentive programs.

It enables Trend Micro to extend its internal research teams by leveraging the methodologies, expertise, and time of external researchers, and protect customers while an affected vendor is working on a patch.

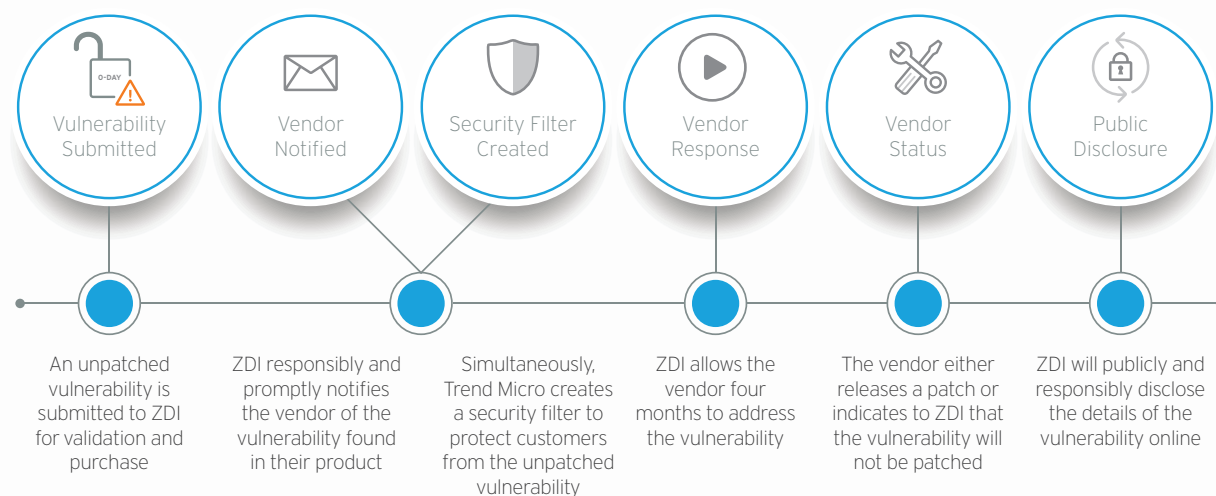


The Zero Day Initiative is the world's largest vendor agnostic bug bounty program and the leader in global vulnerability research and discovery

SINCE 2007<sup>1</sup>

### ZERO DAY INITIATIVE

- 1,453** vulnerabilities published in 2020
- 7,500+** vulnerabilities published since inception
- Over \$25 million USD** awarded since inception
- 81 days** average preemptive protection for Trend Micro™ TippingPoint™ customers ahead of vendor patch in 2020
- A top provider** of vulnerabilities to ICS-CERT, Adobe and Microsoft



### 2020 Global Public Vulnerability Research Market

In their report, "Quantifying the Public Vulnerability Market: 2021 Edition", Omdia found the Zero Day Initiative was #1 in vulnerability disclosures in 2020. The report covers vulnerabilities that have been disclosed by public vulnerability reporting organizations.

- 1,378** total number of publicly disclosed vulnerabilities
- 46%** of the 1,059 vulnerabilities categorized as "Critical-Severities" and "High-Severities" were disclosed by ZDI
- 60.5%** of the 2020 publicly disclosed vulnerabilities were disclosed by ZDI
- 69%** of the 439 vulnerabilities across the top three vendors (Adobe, Microsoft, FoxIT) were disclosed by ZDI
- 825** ZDI published the most vulnerabilities in the Critical-, High-, Medium-, and Low-Severities levels
- 66%** of the 350 vulnerabilities across the top three flaw types were disclosed by ZDI

## WITHOUT ZDI,

many vulnerabilities would continue to remain behind closed doors, or sold to the underground market and used for nefarious purposes.

ZDI's long-standing relationships with software vendors and the research community help influence the importance of security in the product development life cycle, leading to more secure products and more secure customers.

