VULNERABILITY INTELLIGENCE REPORTING OVERVIEW

The Vulnerability Intelligence offering is a collection of technical and threat reporting that is intended to provide stakeholders better clarity to make informed decisions regarding the management of their assets. It plays a key role in prioritization of resources and patch/mitigation/version management.

Vulnerability reporting provides actionable intelligence that helps identify the “signal” from the “noise.” As experience tells us: if everything is “critical,” then nothing is critical.

The offering covers all aspects of vulnerabilities affecting information technology (IT) and operational technology (OT) assets, answering these key questions:

- What are the vulnerabilities that exist?
- What vulnerabilities are being exploited in the wild?
- Does Proof of Concept code exist?
- How is it being exploited?
- How does that exploit impact my environment?
- What actions can our customers take to protect themselves?

Mandiant Intelligence collects information and data from a variety of resources to fully scope technical and threat details from the information:

- Robust open-source tracking from hundreds of resources
  - Vendor advisories, security blogs, security news sites, exploit databases, mailing lists, Twitter, Pastebin, and so on
- Unique, world-class underground research capability – 60+ researchers
  - Engagement of actors in their environments
  - Proactive indication of actor interest, proliferation, and use of exploits
- Global network of Trellix appliances
  - Real-time feedback on what is occurring across various attack surfaces
- Mandiant Services - Mandiant Consulting and Managed Defense
  - Findings from breach investigations and global services organization representing numerous industries or verticals
- Mandiant original research
  - Zero-day discovery and technical analysis

For more information about exploring vulnerabilities in the Mandiant Advantage Threat Intelligence (MATI) platform, see **How to Explore Vulnerabilities (https://docs.mandiant.com/home/mati-how-to-explore-vulnerabilities)**.

Process

Once information has been identified, analysts determine whether to create a new report or update an existing report. Higher priority is given to new information, exploitation-related activity, and higher risk issues.

While some data can be automatically ingested, all vulnerability reports are individually scored and analyzed by one of our expert vulnerability analysts. There are multiple reasons why we approach analysis in this way:

- Ensure that data provided by sources is accurate and reliable
- Determine ratings and field options
- Use historical knowledge of vulnerabilities and targeted products to provides additional context for vulnerabilities with few to no details, including potential impacts, attack vectors, and remediations

Reports have added threat context and focus on exploitation. It is important for customers to understand what *is* happening, not just what *could* happen. When possible, our analysts tie activity back to associated actors, groups, and malware, as well as providing high-level targeting information.

Our vulnerability experts perform in-depth analysis and provide situational awareness on high-risk, critical-risk, and high-profile vulnerabilities. When possible, testing of PoC code and exploit code is performed, and analysis provided from company-wide experts is used throughout. There is a continuous recalculation of all ratings and information contained in our reports.

Definitions

Mandiant Intelligence uses its own Proprietary Ratings within Vulnerability Reporting. Below are definitions for these rating categories and the individual ratings.

Exploitation Rating: Mandiant Intelligence's Exploitation Rating is an indication of what is occurring in the wild in terms of exploitation-related activity. This may drive prioritization when operationalizing the Vulnerability reporting structure into a Security Operations Center (SOC).

- **No Known:** No known exploitation activity, underground discussions, PoC, or exploit code, but has low potential for exploitation.
- **Available:** Exploit or PoC code is publicly available or underground discussions, alleged selling, or alleged privately held code observed.
- **Confirmed:** Limited reported or confirmed exploitation activities.
- **Wide:** Exploitation has been reported or confirmed to widely occur.

Risk Rating: Mandiant Intelligence's Risk Rating is our expert assessment of what impact attackers could have on a targeted organization if they were to exploit a vulnerability.

- **Low:** Exploitation of these vulnerabilities would have little to no security impact on targeted systems. This means that while technically a vulnerability, there is little to no direct security impact an attacker can have on the targeted system or network. Reliability of exploitation is likely low and unlikely to be performed on a wide scale.
- **Medium:** Exploitation of these vulnerabilities would either enable attackers to perform additional activities on the targeted device or network or could allow enable attackers to have a direct impact on the security of the targeted device or network, but would require notable additional factors to be performed or mitigated. Reliability of exploitation is likely questionable and may or may not be able to be performed on a wide scale.
- **High:** Exploitation of these vulnerabilities would enable attackers to have a notable direct impact to the security of targeted devices and networks without needing to overcome any major mitigating factors. Reliability of exploitation is expected to be high and can typically be done on a wide scale.
- **Critical:** Exploitation of these vulnerabilities fundamentally undermine the security of affected devices and networks, enabling actors to perform significant attacks with minimal effort, impacting a wide number of systems, often with little to no mitigating factors to overcome. Reliability of exploitation is most likely very high and can almost certainly be performed effectively at scale.

Source Priorities

- In terms of source priorities, analysts refer to the following list when making decisions on which sources in the queue to write-up first (where possible, and within reason, secondary prioritization may be based on risk rating for existing reports):

    - New vulnerabilities
    - Exploitation Activity
    - Exploit/PoC code Availability
    - Vendor fixes
    - Source(s)
    - Secondary prioritization based on Risk and Exploitation Ratings for existing reports

- Key Vulnerability/Technical Details list
    - CVE
    - Date of Disclosure
    - Vulnerable Vendor, Product, Version, and Components
    - Vulnerability Type
    - Exploitation Consequences
    - CVSS Metrics
    - Patch/mitigation availability
    - Vulnerable Products

Analysis Walkthrough

Often times, there is insufficient data to properly assess the risk or threat a vulnerability poses to an organization. Therefore, our Mandiant Intelligence experts perform additional analysis on the publicly and privately available information to do the following:

- Fill in the gaps of the vulnerability/technical details list with likely information
- Determine what causes the vulnerability to exist
- Ascertain what the vulnerability could be used to do
- Describe how an attacker can successfully exploit this vulnerability
- Determine impact that a successful exploitation could have on a targeted organization
- Identify tips for identifying malicious activity
- Locate which exploits or proof-of-concept codes are available, publicly or privately, analyze to see how they work, and what can they be used to do.
- Provide known exploitation activities, including basic attribution and targeting
- Provide risk rating justifications
- Describe and define ratings – which ratings are based on details AND analysis
    - Exploitation Ratings are almost purely based on our own observations in the underground and customer attack surfaces; however, trusted partners and vendors do provide some indication of activity in the wild
    - Risk Ratings are typically determined based on a combination of the publicly available vulnerability/technical details and the analysis provide by our analysts to fill in the gaps