EXPLORE VULNERABILITIES

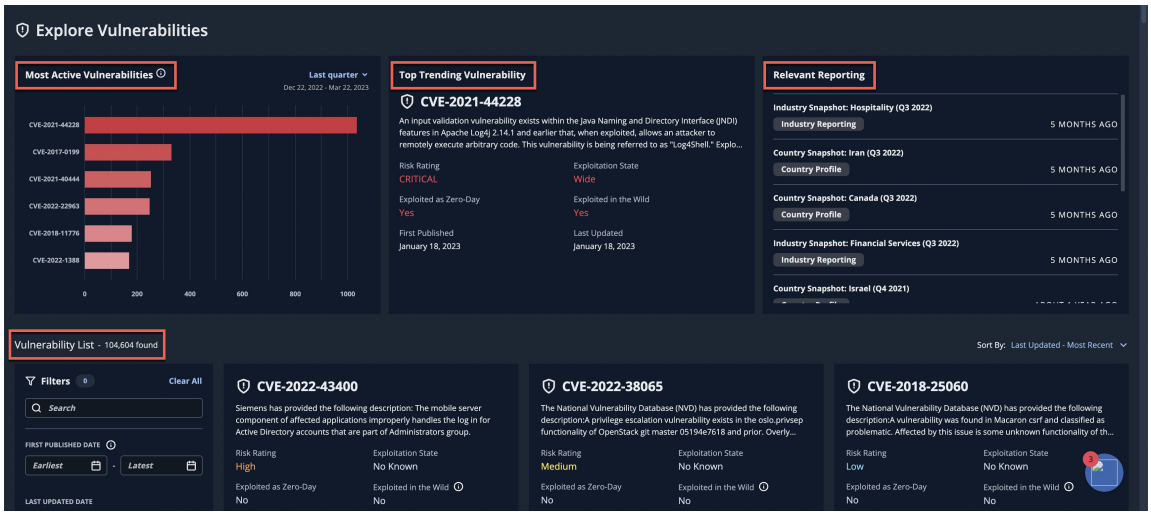
Mandiant Advantage Threat Intelligence (MATI) helps you prioritize patching and mitigation efforts by providing empirical risk scoring, highly contextualized correlations to other indicators of compromise (IOCs, or simply "indicators"), and continuously updated reporting for Vulnerabilities.

Explore Vulnerabilities

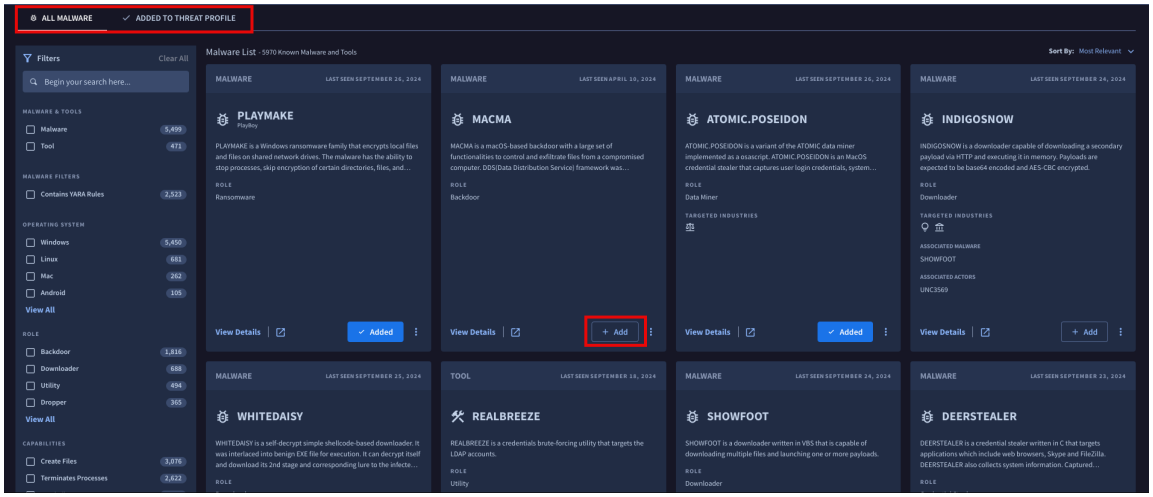
1. To explore Vulnerabilities, click **Explore > Vulnerabilities**.
2. The **Explore Vulnerabilities** dashboard displays the following:
    - **Most Active Vulnerabilities**: The most prolific Vulnerabilities being tracked by Mandiant.
    - **Top Trending Vulnerability**: The Vulnerability that currently has the most appearances within sources such as industry reporting, public and underground discussion groups, and blogs that are monitored by Mandiant.
    - **Relevant Reporting**: The latest reports generated by Mandiant that are related to or explicitly mention the **Top Trending Vulnerability.**

      All Relevant Reports can be downloaded as PDFs.

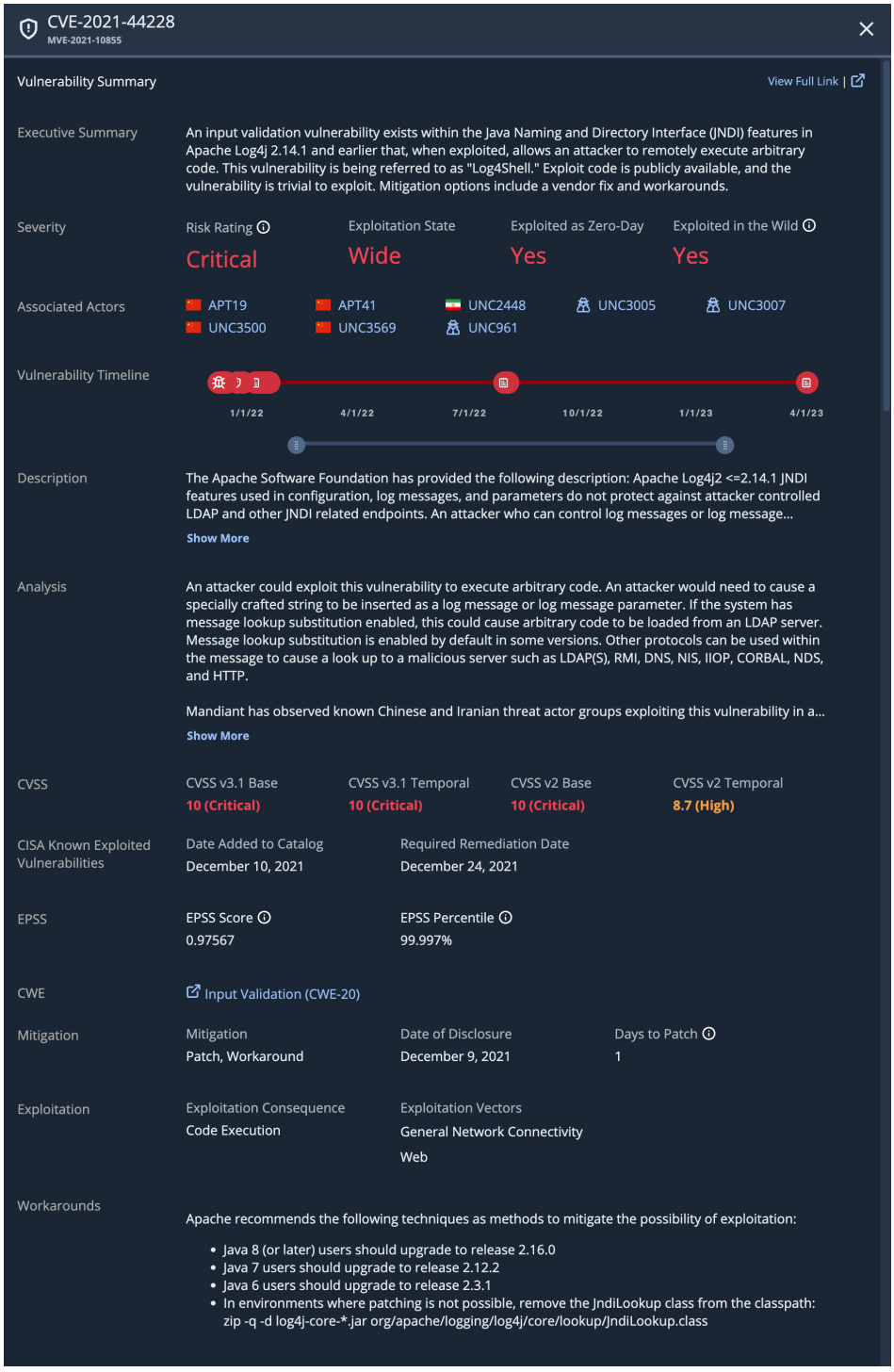
    - **Vulnerability List**: A **filterable** and sortable list of over 100K Vulnerabilities being tracked by Mandiant.



3. Click **Add** for any Vulnerability in the **All Vulnerabilities** tab to monitor ongoing changes to that Vulnerability profile over time, including new activity, associations, or reporting.
    - Navigate to **Added to Threat Profile** to view all the Vulnerabilities added to your Threat Profile.

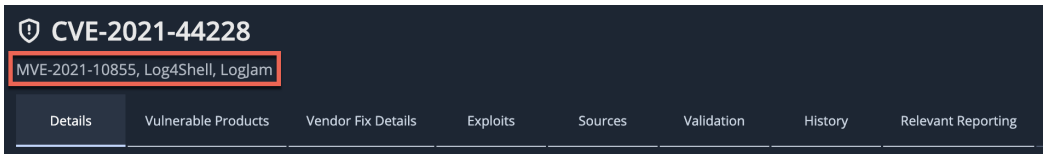


4. Click a specific Vulnerability to view the **Vulnerability Summary.**



4. Click **View Full Link** to explore the complete Vulnerability profile across several tabs as detailed in the following bullets.

> Any aliases for the Vulnerability are listed beneath its **CVE ID (https://www.cve.org/)**, including its MVE ID. MVEs are Mandiant's unique IDs for Vulnerabilities, similar to CVEs (Common Vulnerabilities and Exposures).



- **Details**: Displays the same information as the **Vulnerability Summary** with additional contextual visualizations:
  - **Exploit and Risk Ratings**: This chart shows the current state of the Vulnerability in the context of two dimensions:
    - **Exploitation State**: What's occurring in the wild in terms of exploit-related activity.
    - **Risk Rating**: What impact an attacker would have on a targeted organization if exploitation was successful.

  - **Vulnerable Products**: This graph displays the products affected by the Vulnerability, broken down by percentage of total products.

> For Vulnerabilities with a high number of affected products, not all vulnerable products may be included in the display.

  - **Exploit Grades**: This visual displays the state in which the code for a Vulnerability currently exists and its capability.

- **CVSS v3.1 Base** (https://www.first.org/cvss/v3.1/specification-document#Base-Metrics): This metric group represents the intrinsic characteristics of a Vulnerability that are constant over time and across user environments.
- **CVSS v3.1 Temporal** (https://www.first.org/cvss/v3.1/specification-document#Temporal-Metrics): This metric group represents the intrinsic characteristics of a Vulnerability that are constant over time but not across user environments.
- **CVSS v2.0 Base** (https://www.first.org/cvss/v2/guide#2-1-Base-Metrics): This metric group represents the intrinsic characteristics of a Vulnerability that are constant over time and across user environments.
- **CVSS v2.0 Temporal** (https://www.first.org/cvss/v2/guide#2-2-Temporal-Metrics): This metric group represents the intrinsic characteristics of a Vulnerability that are constant over time but not across user environments.

> For more information, see **CVSS Ratings in MATI** (https://docs.mandiant.com/home/mati-cvss-ratings).

- **Vulnerable Products**: Displays a sortable table of all affected products broken down by **Vendor**, **Product**, and **Version**.

> Vulnerable products are described using Common Platform Enumeration (CPE) format, so changes to these records appear in the **History** tab as CPE updates.

- **Vendor Fix Details**: Provides a sortable table of all vendor fixes broken down by **Name** (with links to patch packages), **Source ID**, and **Date of Patch**.
- **Exploits**: Lists code samples and **metasploit** (https://www.metasploit.com/) modules that can be used for proof-of-concept (PoC) testing of this Vulnerability in your environment. These are broken down by **Vendor** (with links to code samples), the associated **Hashes**, **Exploit Reliability**, **Exploit Grade**, **File Size**, and **Release Date**.
  - **Exploit Reliability:** The degree of analysis performed by Mandiant.
    - **Unreviewed**: The exploit has not been reviewed for legitimacy by an analyst.
    - **Reviewed**: Analysts have reviewed the exploit code, but have not tested it.
    - **Tested**: Analysts have tested the code to confirm functionality.
  - **Exploit Grade**: The state in which the code exists and its current capability.
    - **Unevaluated**: The exploit has not been evaluated by an analyst. This is used when an exploit is ingested through automation and is the only grade automation can assign.
    - **Proof-of-Concept**: This code is intended to demonstrate that exploitation of the Vulnerability is possible and can potentially deploy a non-payload. Non-payload examples include opening the calculator or a raw request that can trigger the Vulnerability without any consequences. The

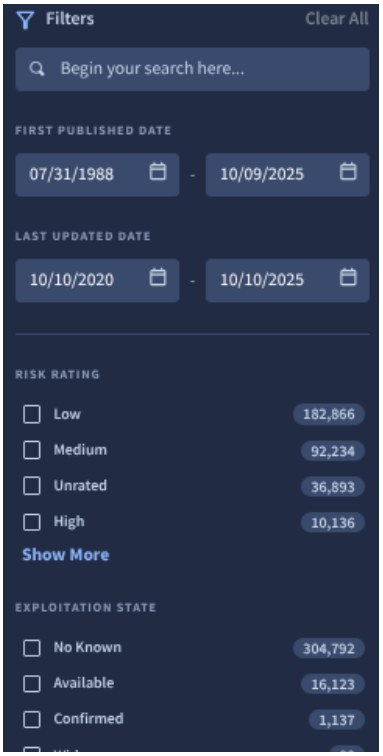
entry has limited or no functionality in its current state, and further development must be made for exploitation to occur.

- **Non-Weaponized**: The code can perform exploitation; however, it does not come weaponized by default. It can exploit the Vulnerability; however, an external payload (which is not part of the code) must be specified to carry out the malicious actions. This may also pertain to exploit code with no predefined code or command to execute upon exploitation, but contains all of the logic required to execute the code or command when the user defines them.
- **Weaponized**: This code contains a malicious payload or specific code or command to perform malicious actions against a vulnerable system. Examples include overwriting or reading a critical file, spawning a reverse shell, deploying known malware, or causing a Denial-of-Service (DoS) condition. The code can typically be used as-is and does not require further development to perform malicious actions.
- **Scanner**: A scanner does not deploy any malicious payloads against a target. Instead, it determines whether the target is exposed to a given Vulnerability and reports this back to an operator. While some scanners do execute a payload (such as running the `whoami` command), execution of the payload is not the goal but rather to determine if the system is vulnerable.
- **Fake**: The code is intentionally fake or misleading. This can be done by researchers attempting to determine which vendors are reporting on unanalyzed exploit code, or by malicious actors attempting to distract researchers. There is no legitimate functionality, and the code may not even pertain to the Vulnerability in question.

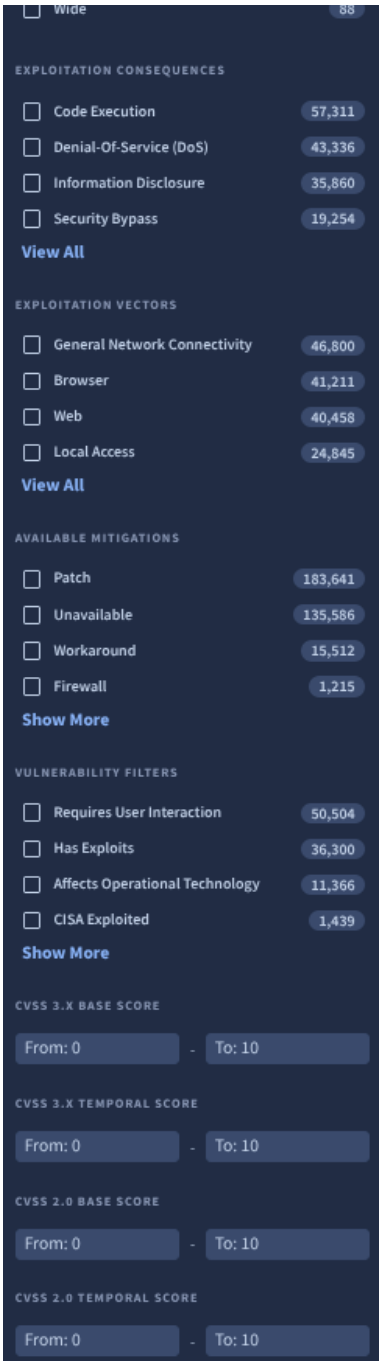
- **Sources**: Provides links to external sources for additional Vulnerability advisories and reports, broken down by **Source**, **Source ID**, **Source Name**, and **Publish Date**.
- **Validation**: Displays Security Validation Actions that can be used to test your security tools against this Vulnerability, if available.
- **History**: Lists **Version Notes** and associated **Dates** for updates to this Vulnerability record by Mandiant.
- **Relevant Reporting**: The latest reports generated by Mandiant that are related to or explicitly mention the selected Vulnerability.

Filtering Vulnerabilities

1. Go to **Explore > Vulnerabilities**.
2. In the **Filters** pane, select the desired filters based on the following options:
   - **First Published Date**: Date when information on the Vulnerability was first made available to Mandiant customers.
   - **Last Updated Date**: Date when Mandiant last published updates regarding the Vulnerability.
   - **Risk Rating**
     - **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 attackers to have a direct impact on the security of the targeted device or network. These Vulnerabilities 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.
     - **Unrated**: Some Vulnerabilities do not have a Mandiant risk rating but do have the other Vulnerability intelligence context included.



This is usually because there is insufficient information to determine the risk rating, or it's still being analyzed.
    - **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 undermines the security of affected devices and networks. These vulnerabilities enable 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.



- **Exploitation State**
    - **No Known**: The Vulnerability has been disclosed by the vendor and published, but Mandiant has no reported instances of exploitation.
    - **Available**: The Vulnerability has been disclosed by the vendor, released, and published, but Mandiant has no reported instances of exploitation.
    - **Confirmed**: Mandiant has observed or has received confirmation from a reliable source that the Vulnerability has been successfully exploited in a limited capacity.
    - **Wide**: Mandiant has observed or has received confirmation from a reliable source that the Vulnerability has been successfully exploited on a large scale.
- **Exploitation Consequences**
    - **Code Execution**: Malicious code is injected and executed by the targeted application.
    - **Denial-Of-Service (DoS)**: A machine, service, or network is temporarily or permanently rendered unavailable to intended users, typically by flooding it with traffic.
    - **Information Disclosure**: A system fails to protect sensitive and confidential information from exposure.
    - **Security Bypass**: The authentication or other security mechanisms of a device or system are circumvented to enable unauthorized access.
    - **Data Manipulation**: Data is inserted, deleted, or altered to hide activities, influence outcomes, or disrupt operations.
    - **Command Execution**: Malicious commands are executed by the host operating system, typically using the privileges of the target application.
    - **Privilege Escalation**: A Vulnerability is exploited to enable elevated privileges to access resources that would otherwise be protected.
    - **Data Loss**: Data is exfiltrated or wiped from the target system.
- **Exploitation Vectors**
    - **Email**: An attacker could exploit the Vulnerability using a maliciously crafted email.
    - **File Share**: A malicious, specially crafted file in a file share could be used to exploit the Vulnerability.
    - **General Network Connectivity**: Exploitation can be conducted over remote access over a computer

network with a vulnerable system.
    - **Local Access**: Exploitation requires direct login access or command shell access to the target system.
    - **Local Network Access**: Attackers could exploit the Vulnerability on another system if they are on the same local network.
    - **Open Port**: Exploitation can occur over exposed ports, whether due to misconfigurations or poor security practices.
    - **Physical Access**: Direct, physical access to a vulnerable system is required to exploit the Vulnerability.
    - **Web**: Exploitation can occur by a user visiting malicious or compromised websites.
- **Available Mitigations**
    - **Anti-Virus Signatures**: Anti-virus signatures capable of detecting exploitation attempts exist.
    - **Firewall**: Specific firewall rules can be used to prevent exploitation attempts.
    - **Intrusion Prevention Signatures**: Intrusion prevention signatures exist capable of preventing exploitation attempts.
    - **Patch**: Vendor fixes exist that mitigate the Vulnerability.
    - **Unavailable**: No mitigations are known to exist.
    - **Workaround**: A solution exists that can mitigate some exploitation attempts, but is not intended to be a full or permanent fix.
- **Vulnerability Filters**
    - **Requires User Interaction**: The Vulnerability can only be exploited with the direct interaction from a potential target.
    - **Has Exploits**: The Vulnerability is known to have exploit or proof-of-concept (PoC) code available, which could potentially be used for exploitation activity.
    - **Affects Operational Technology**: The Vulnerability is known to affect operational technology (OT) and/or industrial control systems (ICS).
    - **CISA Exploited**: The Vulnerability appears in the **Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)** of the Cybersecurity & Infrastructure Security Agency (CISA).
    - **Ovserved In The Wild**: Mandiant has either observed malicious exploitation of a Vulnerability or has received information regarding confirmed exploitation from a reliable or confirmed source.
    - **Zero Day**: The Vulnerability was known to be exploited prior to a patch being made available.
- **CVSS 3.x Base Score (https://www.first.org/cvss/v3.1/specification-document#Base-Metrics)**: Filter based on a range of CVSS 3.1 Base Score metrics.
- **CVSS 3.x Temporal Score (https://www.first.org/cvss/v3.1/specification-document#Temporal-Metrics)**: Filter based on a range of CVSS 3.1 Temporal Score metrics.
- **CVSS 2.0 Base Score (https://www.first.org/cvss/v2/guide#2-1-Base-Metrics)**: Filter based on a range of CVSS 2.0 Base Score metrics.
- **CVSS 2.0 Temporal Score (https://www.first.org/cvss/v2/guide#2-2-Temporal-Metrics)**: Filter based on a range of CVSS 2.0 Temporal Score metrics.

Vulnerabilities Overview

The following video provides a quick overview of navigating the Vulnerabilities web interface:

Vulnerabilities Deep Dive

The following recording from one of our Principal Architects provides a deep dive into getting the most from Mandiant's Vulnerability intelligence: