MANDIANT
NOW PART OF Google Cloud

ATTACK SURFACE MANAGEMENT
WHITE PAPER

Insights Into the External Enterprise Attack Surface

The content in this document was originally published in The Defender's Advantage Cyber Snapshot Issue 2.

Issue data referenced in this document is directly sourced from Mandiant Advantage Attack Surface Management, spanning 30,904 Collections. Collections define the scope of assets discovered and monitored by Attack Surface Management, yielding an enumerated inventory of external assets, applications and services and identified issues. The data set includes 6,022,027 issues identified from January 1, 2022, to June 30, 2022, 62,135 with issues of high or critical severity. Issues are a subset of Collections, which contain the asset inventory and associated technologies running on external attack surfaces. Issue severity is assigned based on the potential impact to the affected system. In situations where common vulnerabilities and exposures (CVE) are identified, the severity is tied to the Risk Rating from Mandiant Advantage Threat Intelligence.

An organization's digital footprint evolves organically through the adoption of cloud, new applications, devices and business relationships. Unfortunately, digital growth does not always occur under the purview of security or IT teams, commonly called shadow IT. This increases the risk of misconfigurations or applications and services receiving permissions that violate company security policies. From frontline observations and data gathered from the Mandiant Advantage platform, Mandiant has composed best practices for establishing and incorporating comprehensive attack surface management programs into cyber defense.

Quantifying the average external attack surface

The enterprise attack surface is comprised of devices, applications, services, libraries, people and partners, all of which can serve an exploitable entry point for a threat actor. Threat actors can use any vectors exposed to the internet to perform reconnaissance, move laterally, maintain access or achieve their overall mission.

Mandiant observed the following external attack surface trends over a six-month period associated with the "average" Collection:

- 2,746 exposed assets discovered, including DNS records, URLs, network services, AWS S3 buckets, GitHub repositories, mail servers and more
- 244 unique technology vendors and business relationships
- 13 unique applications with 150 instances of applications actively being used
- 9 unique supply chain service vendors with 102 instances of supply chain services being used
- Approximately 50% are multi-cloud, with usage across a combination of Microsoft Azure, Google Cloud Platform and AWS

Software supply chain and supply chain services

The largest Collections analyzed by Mandiant have more than 58 supply chain service vendors and over 1,200 unique instances of supply chain services detected at the external edge. Each vendor has a connection to the organization's infrastructure and is part of the larger supply chain ecosystem. As a best practice, Mandiant recommends performing an audit of all partners, along with SaaS and supply chain providers, being mindful of the criticality of the assets they interact with to assess the organization's potential risk. Mandiant M-Trends 2022[1] reported 17% of intrusions investigated by Mandiant came from supply chain compromise, highlighting the importance of integrating a strong supply chain management program into cyber defense operations.

Mapping assets to relevant applications and services provides insight into business relationships that a security team may not be aware of, including third- and fourth-party suppliers. CISA[2] recommends identifying upstream suppliers, or the suppliers' sources that can disrupt the broader ecosystem if breached. There are different types of supply chain vendors to account for, including commercial-off-the-shelf software (COTS), software-as-a-service (SaaS), and open-source software (OSS), as well as network infrastructure providers, physical infrastructure providers and parts suppliers.

1. Mandiant (2022). M-Trends 2022 Report.
2. CISA. SCRM Essentials: Information and Communications Technology Supply Risk management (SCRM) in a Connected World.

Database exposures

Mandiant found 4.65% of Collections analyzed had databases exposed to the internet from January 1, 2022 to June 30, 2022. The Collections with database exposures saw 36 unique exposures on average, which implied underlying systemic issues that allowed these exposures.

Database exposures are high risk vectors, due to the potentially high volume of sensitive and confidential information that could be leaked. Organizations that identify database exposures should take immediate action to secure these assets, block common database ports, monitor cloud account access and perform a thorough investigation to assess the data sensitivity levels, identify any unauthorized access (if sufficient logging data is available) and the impact of the data exposure.

Critical severity, high priority

While it remains important to establish visibility into the enumerated asset inventory, technology vendors and related vulnerabilities, it's even more important to prioritize hardening and remediation efforts on the vectors that present the most risk. Mandiant recommends organizations prioritize critical and high severity issues, including CVEs with common vulnerability scoring system (CVSS) scores greater than 7.0 and focus on CVEs that have been or are likely to be exploited in the wild. Issues discovered by Attack Surface Management include vulnerabilities, misconfigurations, indicators of compromise (IOCs) or a data leak of any sort.

From January 1, 2022, to June 30, 2022, Mandiant identified over six million issues across small organizations and large enterprises. Of these, 62,135 (1.03%) were critical or high severity.

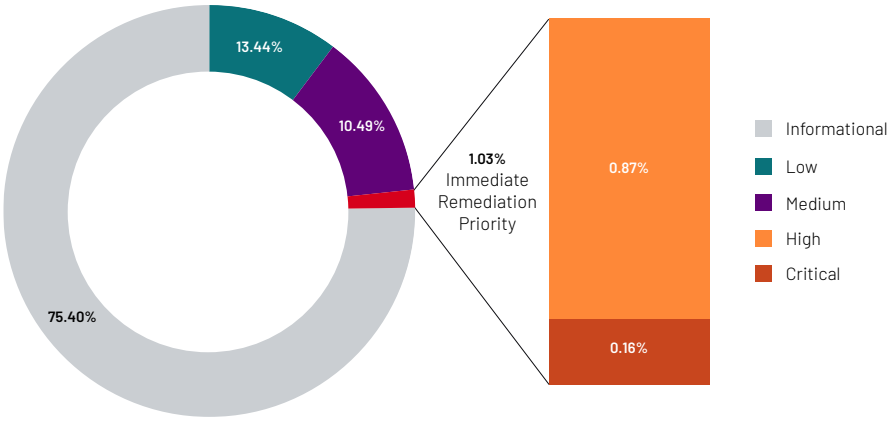

Figure 1. Issues observed by Mandiant Advantage Attack Surface Management from January 1, 2022 to June 30, 2022, assigned by severity.

An issue is a finding discovered on an external asset that warrants further investigation.

Issues are identified and confirmed by testing known vulnerabilities and exposures. Organizations should remediate and patch the top five Critical Severity Issues (Table 1) immediately.

TABLE 1: Top 5 Critical Severity Issues identified by Mandiant Advantage Attack Surface Management from January 1, 2022 to June 30, 2022.

Rank	Critical issue	Exploited in the wild	Potential impact	Remediation recommendation
1	Wordpress Configuration Information Leak	No	PHP configuration files can contain sensitive information, such as database host and name, username, password and security keys. Any number of those data points can be leveraged in conjunction with other information gathered during the reconnaissance process to further the mission of a threat actor.	1. Audit the contents of the configuration file to determine if sensitive information was exposed. 2. Set permissions on the configuration file to prevent anonymous users from being able to read it.
2	Drupal Remote Code Execution (CVE-2019-6340)	Yes	Some field types do not properly sanitize data from non-form sources in Drupal 8.5.x before 8.5.11 and Drupal 8.6x before 8.6.10. When exploited, a threat actor can remotely execute arbitrary PHP code. The proof-of-concept is publicly available and there are reports of exploitation in the wild. CISA added the vulnerability to the Known Exploited Vulnerabilities Catalog and required a remediation date of April 15, 2022.	1. Disable all web service modules or configure the web server to not allow GET/PUT/PATCH/POST 2. Apply Drupal Security Update[3]
3	Microsoft Exchange Server Remote Code Execution (CVE-2021-31206)	No	An attack could exploit a traversal vulnerability that exists within the parsing of CAB files, allowing them to execute arbitrary code. However, exploitation requires adjacent network access and user interaction.	1. Follow the guidance provided by Microsoft-(50004778) Security Update Information[4] 2. Restrict egress communications from the Exchange Server 3.Restrict lateral movement portal for internal communication paths (SMB, WMI, RDP) 4. Restrict privilege account
4	SAP Memory Pipes Desynchronization (CVE-2022-22536)	No	An authenticated threat actor could prepend a user's request with arbitrary data, essentially impersonating the user or poisoning intermediary Web caches. A successful attack could result in complete compromise of Confidentiality, Integrity and Availability of the systems. A proof-of-concept is publicly available.	1. Apply SAP Security Update[5]
5	Apache HTTP Server-Side Request Forgery (CVE-2021-40438)	Yes	An attacker could send a specially crafted HTTP request to forward arbitrary network requests to an attacker-specified endpoint to exploit the service-side request forgery vulnerability in Apache HTTP Server 2.4.48 and earlier. CISA added the vulnerability to the Known Exploited Vulnerabilities Catalog and required a remediation date of December 15, 2022.	1. Perform an audit to find all devices and applications using Apache HTTP Server 2.4.48 and earlier versions. 2. Upgrade

Mandiant previously reviewed the top five critical and high severity Issues[6] commonly found across Collections. Remediation guidance from Mandiant experts can be found in our blog Preventing and Remediating External Asset Exposures.[7]

3. Drupal (February 20, 2019). Drupal core - Highly critical - Remote Code Execution - SA-CORE-2019-003.
4. Microsoft (July 13, 2021). Description of the security update for Microsoft Exchange Server 2013: July 13, 2021 (KB5004778).
5. SAP (February 11, 2022). Remediation of CVE-2022-22536 Request smuggling and request concatenation in SAP NetWeaver, SAP Content Server and SAP Web Dispatcher.
6. Mandiant (2022). The Defender's Advantage Cyber Snapshot, Issue 1.
7. Mandiant (July 2022). Preventing and Remediating External Asset Exposures.

Assess and prioritize at scale

Based on Mandiant observations, many organizations have thousands of internet-facing assets and hundreds of application and service vendors interacting with their attack surfaces. To mitigate the risk of assets or supply chain vendors being used as initial compromise vectors, security teams need to establish and streamline asset enumeration, supply chain management and vulnerability detection. Improving visibility into all aspects of the attack surface informs risk mitigation and enables faster remediation and response times. Consistent visibility into an organization's entire external attack surface and accurate, intelligence-led, risk-based prioritization help ensure that organizations focus remediation activities on the most critical attack vectors.

Read more articles from **The Defender's Advantage Cyber Snapshot**.

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT
NOW PART OF Google Cloud