beazley

Article

Exposed Vulnerabilities

Jad Nehmé • March 01, 2023

An important component of an organization's cybersecurity protocol is to maintain ongoing vigilance when it comes to exposed vulnerabilities. A vulnerability is a weakness or a flaw that allows a threat actor to breach at least one of the three security principles: confidentiality, integrity and availability. Once a security vulnerability is made known, developers and security teams work together to provide a fix, which is called a security patch.

New critical and high-risk vulnerabilities are being discovered and published every day, averaging as many as 15 per day in the first half of 2022. Some of these vulnerabilities were exploited in the wild for years before being discovered by the security community, or before efficient security patches were made available. This makes it very difficult for IT and security teams to keep track and apply security patches before threat actors discover and exploit vulnerabilities. The average mean time to patch is between 60 and 150 days, yet studies showed that some vulnerabilities are identified and exploited by threat actors 5 minutes after being publicly disclosed.

Moreover, regardless of whether software components are patched or not, some applications are vulnerable due to insecure software development practices, use of compromised development libraries and packages, or weak security configurations, especially in cloud environments (with the common misassumption that these environments are "secure by default").

The impact of a successful exploitation of a vulnerability can vary from disclosing technical data or causing a denial of service to fully compromising a system, which often leads to a network infiltration. Fortunately, there are things that organizations can do to protect against these attacks.

BUILD SYSTEMS WITH 'SECURITY BY DESIGN'

Several practices can help reduce the number of vulnerabilities in your systems. First, train your developers and programmers on security practices and provide them with security source code review tools. Second, define a strategy for using and tracking open-source libraries

and code. And finally, define configuration hardening guidelines for your most used and critical asset types (especially for cloud resources).

REDUCE YOUR ATTACK SURFACE

A good way to protect your assets is by not exposing them to the internet. This is particularly valid for remote administration and management protocols. Ideally, this means limiting the access to employees connected to your corporate network, by either being physically on-premise or by using secure remote connection procedures (e.g. a VPN with MFA). This also applies to accessing sensitive applications and projects in development or test environments where configuration or backup files may be easily accessible. In some cases where a VPN is not an option, limiting connections to specific predefined source IP addresses can also help limit your attack surface.

IDENTIFY VULNERABILITIES BEFORE THREAT ACTORS DO

There are several methods to identify vulnerabilities. Some of them can be automated, while others require manual interventions from specialized security professionals. Ideally, an organization will utilize a combination of methods, including automated regular vulnerability scans (if possible monthly), penetration testing by specialized professionals (starting with sensitive applications), bug bounty programs, daily or automated security watch and vulnerability hunting.

REDUCE THE LIKELIHOOD OF A SUCCESSFUL EXPLOITATION

To reduce the likelihood of threat actors exploiting vulnerabilities or compromising systems, an organization has a number of options. The most critical is to ensure immediate action to applying security patches or other adequate protection, such as temporarily limiting internet exposure, or putting the service behind a properly configured WAF in blocking mode. Organizations are also advised to deploy EDR with automatic remediation enabled on servers exposed to the Internet. This can stop some exploitation attempts in their tracks. And finally, harden the configuration of your servers that may be exposing services and applications on the internet. This includes disabling or hiding unnecessary or insecure services and features such as obsolete protocols.

LIMIT THE IMPACT OF A SUCCESSFUL EXPLOITATION

Successful exploitation of a vulnerability would not necessarily lead to a full compromise of a server or to lateral movement within the network. There are many controls that an organization can implement to limit the impact of successful exploitation of a vulnerability exposed to the internet, including the use of a three-tier application architecture with a DMZ for servers exposing services to the internet, internal network segregation for different asset types, and limiting and controlling servers' outbound access to the internet. Organizations are also encouraged to configure permissions in alignment with the principles of least privilege.

According to Palo Alto Networks, Inc.'s Unit 42 research, 99% of cloud users, roles, services and resources are granted excessive permissions.

As a start, this can be addressed by segregating administration groups and limiting their scope. This can be achieved by using an Active Directory (AD) tiering model or Microsoft's enterprise access model, for example. Domain administrators should not be allowed to connect remotely to high-risk assets like servers exposing services to the internet, and no services should be running using domain admin privileges on these high-risk assets. Use purpose-dedicated service accounts with the least privilege principle to ensure that permissions do not prove to be a concern.

Consider implementing security hardening and restrictions on exposed services to ensure there is no execution of scripts or unsigned software (ex. aligning to the CIS benchmark recommendations), or preventing access to the Local Security Authority Server Service (Lsass) process that stores users' passwords locally on endpoints by applying credential guard, reducing the number of locally cached credentials to 2, and running Lsass as protected process light (PPL) PPL.

Also, make sure you change default credentials, especially for built-in administration/management accounts (ex. iLO and iDRAC ports). There is no one single activity or protocol that can completely protect your organization against the possibility of a cyberattack. But by taking a multi-pronged approach to identifying and addressing exposed vulnerabilities, your system and assets will be far better protected.

Jad Nehmé

Client Experience Manager

Opinions expressed here are the author's own.

beazley