Glossary of Terms

unauthenticated attack: An attack that does not require authentication to the vulnerable device prior to carrying out the attack. This metric does not gauge the strength or complexity of the authentication process, only that an attacker is not required to provide credentials before an exploit may occur.

authenticated attack: An attack where credentials that exist must be provided prior to the attack. These credentials can be of any strength or complexity and exist either locally on the vulnerable device or on a remote authentication database.

network attack: An attack that must be bound to the network stack, and one or more layer 3 hops must separate the source of the attack and the destination of the attack. A network attack could originate from any routable origin, including networks internal and external to an organization. Proper access controls will mitigate but not completely prevent the attack.

adjacent attack: An attack that originates from the same layer 2 domain as the victim device. Examples of local networks include Bluetooth, 802.1x, and IEEE 802.11.

local attack: An attack on a vulnerability that is not bound to the network stack and the attacker’s path is via read/write/execute capabilities. Additionally, the attacker exploits the vulnerability by accessing the target system locally (e.g., keyboard, console), or remotely (e.g., SSH); or the attacker relies on User Interaction by another person to perform actions required to exploit the vulnerability (e.g., using social engineering techniques to trick a legitimate user into opening a malicious document). Examples of locally exploitable vulnerabilities are peripheral attacks such as USB Direct Memory Attacks (DMA), and local privilege escalations.

physical attack: An attack that requires the attacker to interact physically with the vulnerable device to successfully attack the device.

denial of service: When a vulnerable system or service is effectively unavailable to users of the system. Examples include an unexpected (crafted) packet causing a system to crash. If a device is performing under conditions that are beyond the upper threshold of the product specifications and the product becomes unavailable and then goes back to normal operating conditions when within specification, Cisco does not consider this a denial of service vulnerability. Therefore, these types of denial of service attacks are not in Cisco Security Advisories.

crafted packet: A packet that has been specifically created or altered after creation by human action. By definition, a crafted packet should not be seen during the normal operation of a network.

malformed packet: A packet that cannot be processed according to specification. These packets are usually discarded. An example of a malformed packet is an IGMP null payload packet that is less than 28

bytes long. A normal IGMP packet consists of a 20-byte IP header and an 8-byte IGMP body.

command injection: An attack where arbitrary commands are sent to the host operating system via a vulnerable application. For example, if a web interface on a router accepts user supplied data (forms, cookies, HTTP headers etc.) and passes it to a system shell. Command injection attacks are mostly due to insufficient input validation.

static credentials: Also called hard-coded credentials and can be any of the following:

plaintext passwordshashed passwordsauthorized keysPEM formatted key filesdefault credentials still enabled in a fully functional system

Static credentials can be used for inbound authentication or outbound communication to external components such as database replication or encryption of internal data. Static credentials are usually high risk because they allow an attacker to bypass standard authentication mechanisms and usage can also be difficult to detect.

privilege escalation: Occurs when privileges are attained beyond what is intended by a system or system administrator. Generally speaking, vulnerabilities that allow privilege escalation allow regular, authenticated users to obtain a privilege or privileges that are usually reserved for administrators or System accounts.

cross-site request forgery: An attack where a victim is tricked into performing actions in an application that the victim is using. For example, if an administrator of a vulnerable application receives a link (via text or email) from an attacker which, when executed, causes a compromise of the application. Examples of a compromise can be a new administrative user created or another configuration change that furthers the attacker’s goals.

SQL injection: These attacks happen when SQL commands are inserted into an application and sent to the SQL database. The intent of the attack can be to reveal database information or cause a denial of service.

container escape: Containers are applications or processes that have their own namespaces. Namespaces may include routing tables, authentication sources and other resources managed by different tenants in a multiple container environment. Important for this definition is the concept of an attacker compromising one container and then expanding the footprint of the attack. For example, an attacker could install a custom container which in turn gains root access on a physical machine or cluster of machines belonging to other tenants.

access control list (ACL): Access control lists, or ACLs, are filtering mechanisms present on many network devices. ACLs may be in a Cisco SA workaround section. ACLs permit or deny network traffic based on the Layer 3 or Layer 4 characteristics of the packet. For example, the following ACL excerpt from a Cisco IOS device denies telnet traffic on TCP port 23, but allows SSH traffic on TCP port 22.

```
access-list 100 deny tcp any any eq 23
access-list 100 permit tcp any any eq 22
```

Once created, ACLs used for traffic filtering are applied to network interfaces in either the inbound or outbound direction.

infrastructure access control list: A technique through which ACLs are applied around the outside of a network. iACLs may be in a Cisco SA workaround section when applicable. Infrastructure ACLs aim to filter incoming network traffic that is targeted to the network itself while allowing all other traffic to travel across the network.

control plane policing (CoPP): A security feature on Cisco IOS devices that permits, denies, or rate limits network traffic to a network device. CoPP filters traffic to a network device, but not through it. In the context of security advisories, CoPP allows us to deny certain, potentially malicious, traffic on a network device without applying an ACL to all interfaces on the device. This single point of application coupled with the characteristic that it only affects traffic to the device makes CoPP a viable mitigation when the device itself has a vulnerability.

Additional Resources

Cisco Security Advisories