Network Security v1.0

/ Securing Networks / Current State of Affairs

Network Security

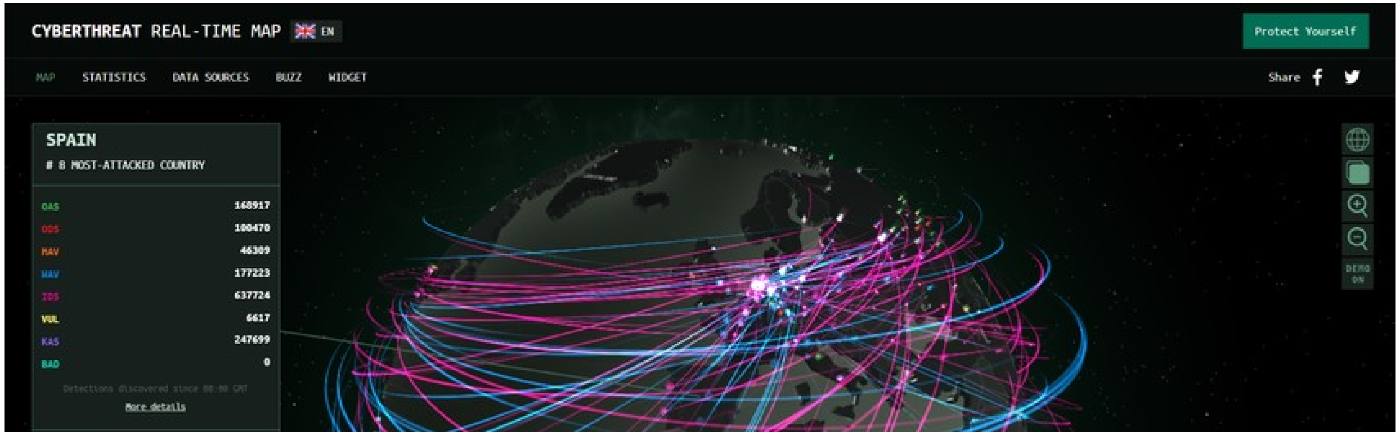
Current State of Affairs

1.1.1

Networks Are Targets

Networks are routinely under attack. It is common to read in the news about yet another network that has been compromised. A quick internet search for network attacks will return many articles about network attacks, including news about organizations which have been compromised, the latest threats to network security, tools to mitigate attacks, and more.

To help you comprehend the gravity of the situation, Kapersky maintains the interactive Cyberthreat Real-Time Map display of current network attacks. The attack data is submitted from Kapersky network security products that are deployed worldwide. The figure displays a sample screenshot of this web tool, which shows these attacks in real time. Many similar tools are available on the internet and can be found by searching for cyberthreat maps.



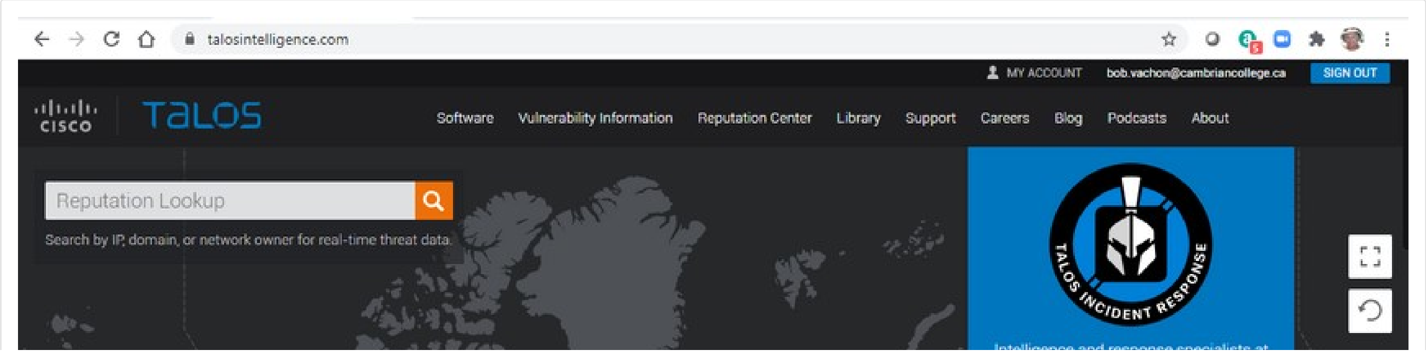
1.1.2

Reasons for Network Security

Network security relates directly to an organization's business continuity. Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people’s privacy, and compromise the integrity of information. These breaches can result in lost revenue for corporations, theft of intellectual property, lawsuits, and can even threaten public safety.

Maintaining a secure network ensures the safety of network users and protects commercial interests. Keeping a network secure requires vigilance on the part of an organization’s network security professionals. They must constantly be aware of new and evolving threats and attacks to networks, and vulnerabilities of devices and applications.

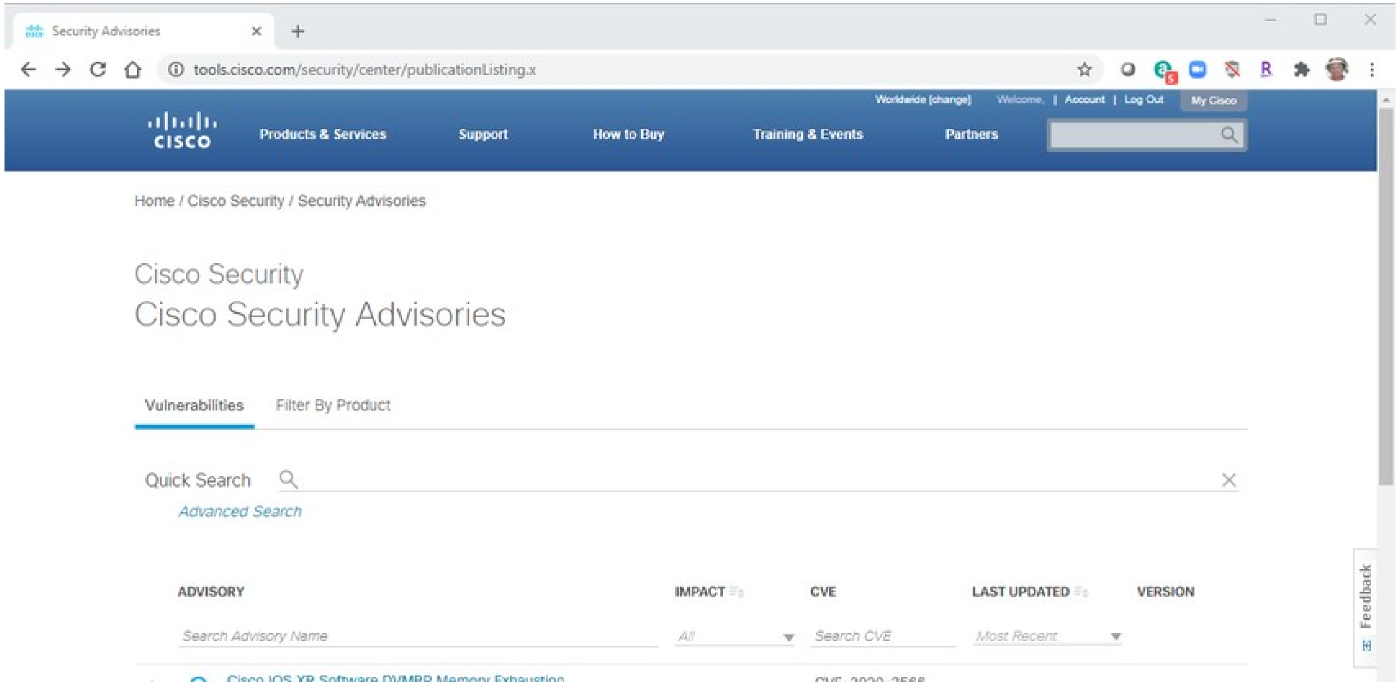
Many tools are available to help network administrators adapt, develop, and implement threat mitigation techniques. For instance, the Cisco Talos Intelligence Group website, shown in the figure, provides comprehensive security and threat intelligence to defend customers and protect their assets.



Search by IP, domain, or network owner for real-time threat data.

intelligence and response specialists at your side.
INTRODUCING
Cisco Talos Incident Response
3
1
8
2
3
2
1
1
1
3
3
2
2
6
1
3
1
1
1
1
5
2
1
67
2
2
2
1
1
+
−

Another group, called the Cisco Product Security Incident Response Team (PSIRT), is responsible for investigating and mitigating potential vulnerabilities in Cisco products. The figure displays a sample Cisco Security Advisories page which lists these vulnerabilities in real time and provides network administrators with information to help mitigate them.



Home / Cisco Security / Security Advisories

Cisco Security

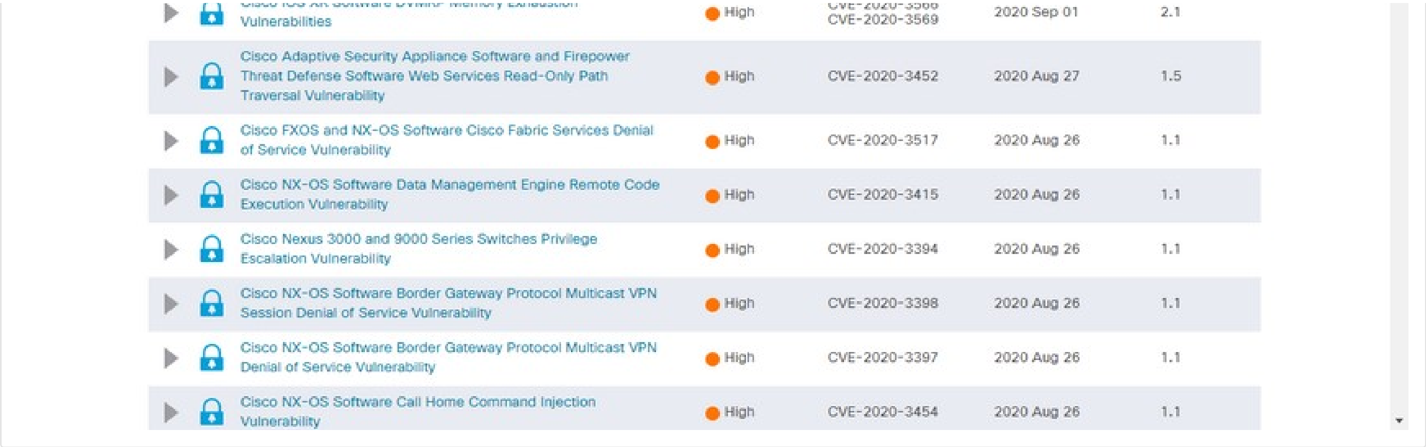
Cisco Security Advisories

Vulnerabilities Filter By Product

Quick Search

Advanced Search

ADVISORY	IMPACT	CVE	LAST UPDATED	VERSION
Search Advisory Name	All	Search CVE	Most Recent	
Cisco IOS XR Software DVMRP Memory Exhaustion		CVE-2020-3566		



Cisco IOS XR Software DVMRP Memory Exhaustion Vulnerabilities	● High	CVE-2020-3566 CVE-2020-3569	2020 Sep 01	2.1
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Read-Only Path Traversal Vulnerability	● High	CVE-2020-3452	2020 Aug 27	1.5
Cisco FXOS and NX-OS Software Cisco Fabric Services Denial of Service Vulnerability	● High	CVE-2020-3517	2020 Aug 26	1.1
Cisco NX-OS Software Data Management Engine Remote Code Execution Vulnerability	● High	CVE-2020-3415	2020 Aug 26	1.1
Cisco Nexus 3000 and 9000 Series Switches Privilege Escalation Vulnerability	● High	CVE-2020-3394	2020 Aug 26	1.1
Cisco NX-OS Software Border Gateway Protocol Multicast VPN Session Denial of Service Vulnerability	● High	CVE-2020-3398	2020 Aug 26	1.1
Cisco NX-OS Software Border Gateway Protocol Multicast VPN Denial of Service Vulnerability	● High	CVE-2020-3397	2020 Aug 26	1.1
Cisco NX-OS Software Call Home Command Injection Vulnerability	● High	CVE-2020-3454	2020 Aug 26	1.1

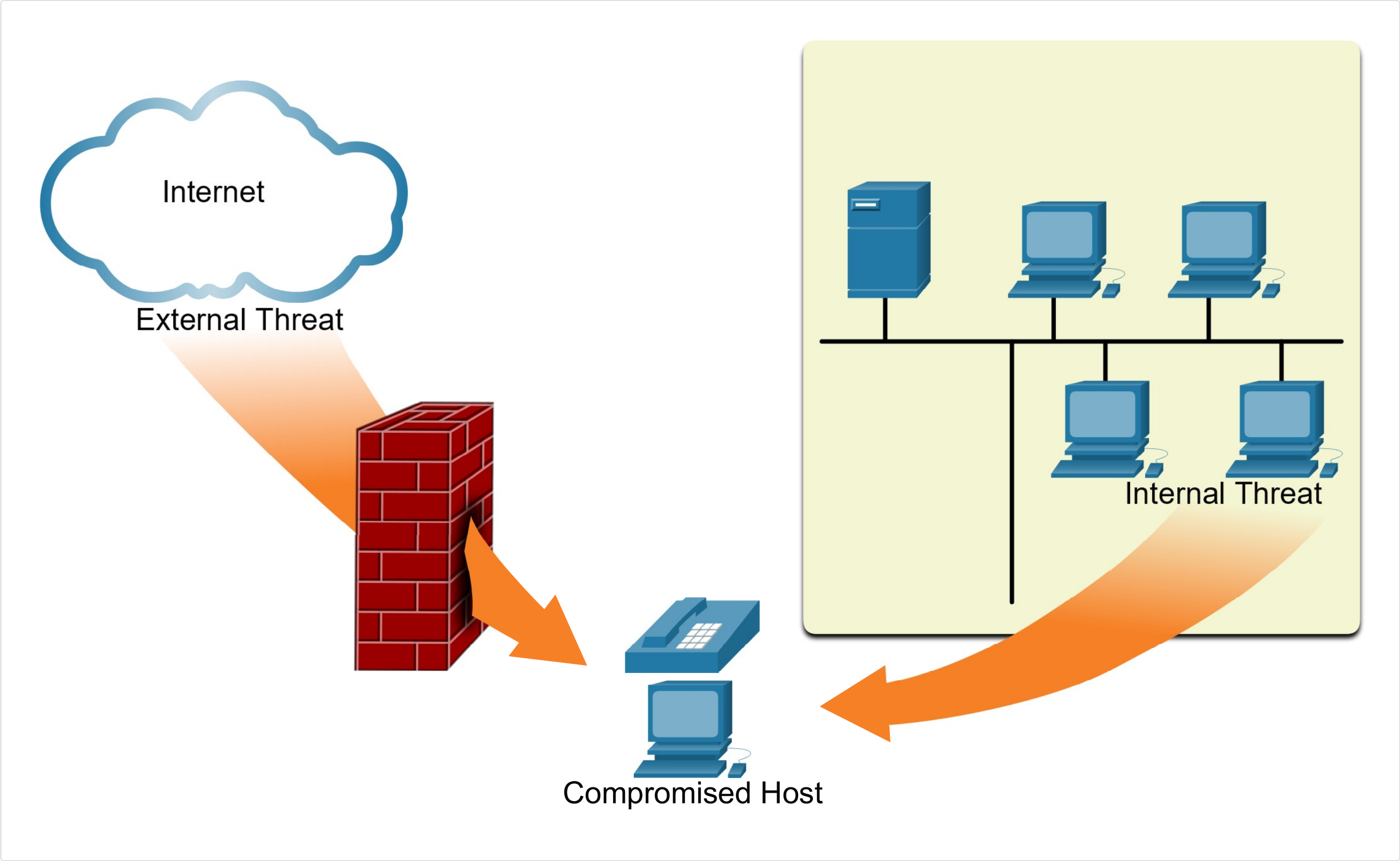
1.1.3

Vectors of Network Attacks

An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network, as shown in the figure. For example, threat actors may target a network through the internet, to disrupt network operations and create a denial of service (DoS) attack.

External and Internal Threats

Network Security



Note: A DoS attack occurs when a network device or application is incapacitated and no longer capable of supporting requests from legitimate users.

An internal user, such as an employee, can accidentally or intentionally:

- Steal and copy confidential data to removable media, email, messaging software, and other media.
- Compromise internal servers or network infrastructure devices.
- Disconnect a critical network connection and cause a network outage.
- Connect an infected USB drive into a corporate computer system.

Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Employees may also have knowledge of the corporate network, its resources, and its confidential data.

Network security professionals must implement tools and apply techniques for mitigating both external and internal threats.

Network Security

1.1.4

Data Loss

Data is likely to be an organization's most valuable asset. Organizational data can include research and development data, sales data, financial data, human resource and legal data, employee data, contractor data, and customer data.

Data loss, or data exfiltration, is when data is intentionally or unintentionally lost, stolen, or leaked to the outside world. The data loss can result in:

- Brand damage and loss of reputation
- Loss of competitive advantage
- Loss of customers
- Loss of revenue
- Litigation/legal action that results in fines and civil penalties
- Significant cost and effort to notify affected parties and recover from the breach

Network security professionals must protect the organization's data. Various Data Loss Prevention (DLP) controls must be implemented that combine strategic, operational, and tactical measures.

Common data loss vectors are displayed in the table.

Term	**Definition**
Email/Social Networking	The most common vector for data loss includes instant messaging software and social media sites. For instance, intercepted email or IM messages could be captured and reveal confidential information.
Unencrypted Devices	A stolen corporate laptop typically contains confidential organizational data. If the data is not stored using an encryption algorithm, then the thief can retrieve valuable confidential data.
Cloud Storage Devices	Saving data to the cloud has many potential benefits. However, sensitive data can be lost if access to the cloud is compromised due to weak security settings.

Network Security

Term	Definition
Removable Media	One risk is that an employee could perform an unauthorized transfer of data to a USB drive. Another risk is that a USB drive containing valuable corporate data could be lost.
Hard Copy	Corporate data should be disposed of thoroughly. For example, confidential data should be shredded when no longer required. Otherwise, a thief could retrieve discarded reports and gain valuable information.
Improper Access Control	Passwords are the first line of defense. Stolen passwords or weak passwords which have been compromised can provide an attacker easy access to corporate data.

1.1.5

Video - Anatomy of an Attack

Network Security

1.0
Introduction

1.2
Network Topology Overview