

Risk Assessment for Cisco

As a Senior Security Architect, you have been tasked with conducting a comprehensive security assessment of a multi-tier web application used by your chosen organization. The application processes sensitive data, integrates with third-party APIs, and runs on a cloud infrastructure. You are free to select any industry or organization as the context (e.g., banking, e-commerce, healthcare).

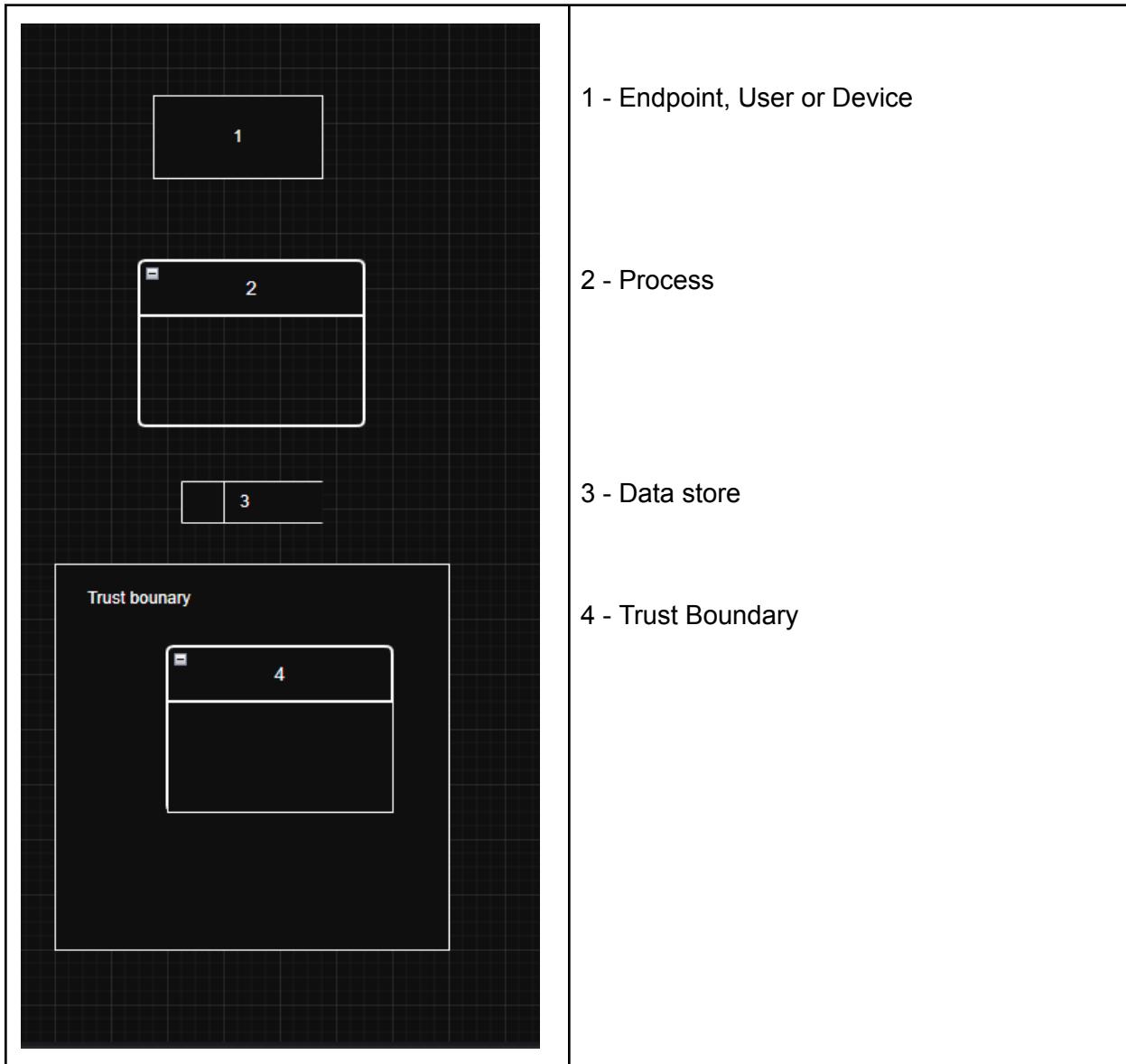
You must create a complete security assessment that demonstrates your ability to think like an attacker while maintaining the perspective of a defender. This is not a checkbox exercise – you need to demonstrate a deep understanding of how threats propagate through complex systems.

Shady Adel Adly Fawzi
20231700320
Cybersecurity level 3

Poula Saber Kyrillos Labib
AI level 3

Abdullah Hany Ahmed Raafat
20231700231
AI level 3

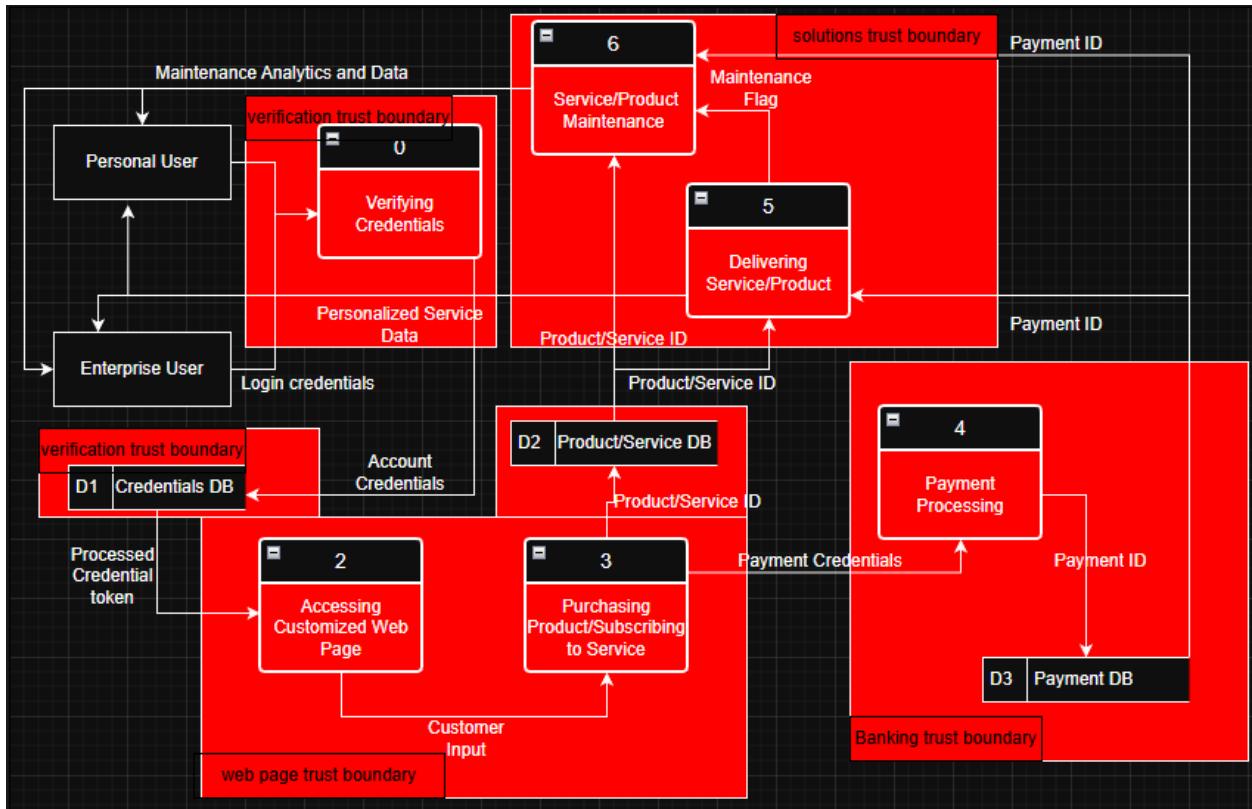
Phase 1: Advanced Threat Modeling



1. Business Logic DFD

Built a general DFD to how business logic between the customers/clients and Cisco would look like. We are assuming that most business transactions and operations would happen through

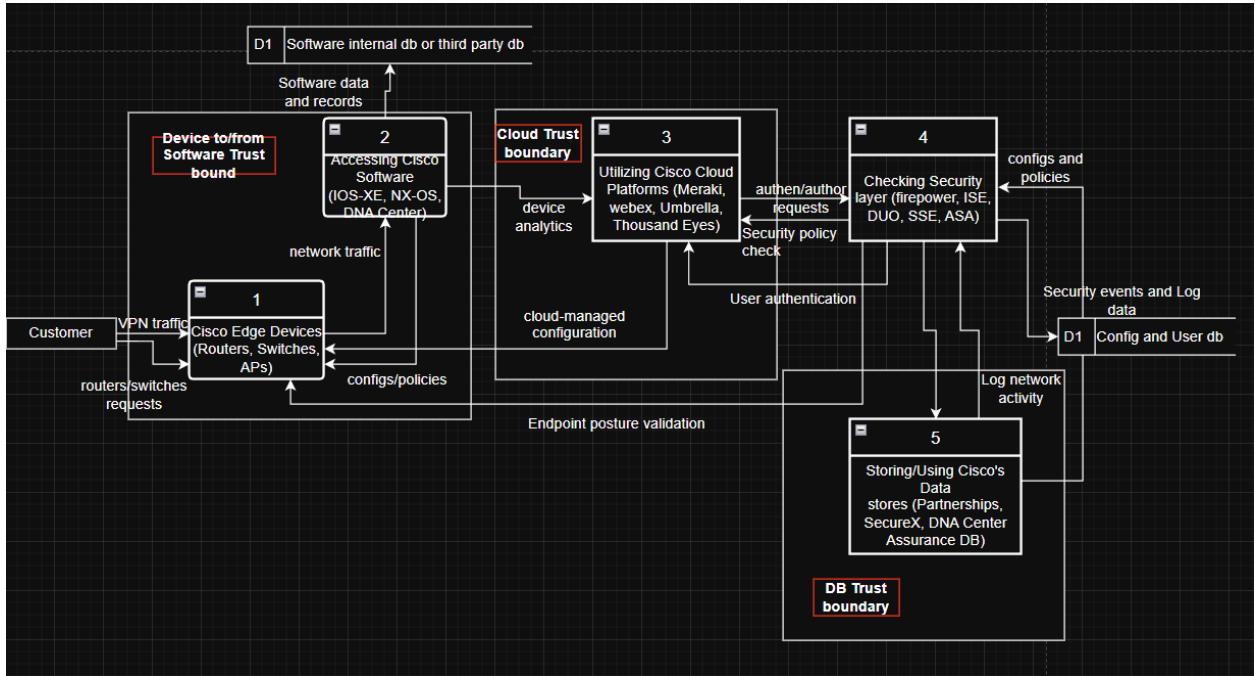
their web page/app where customers can view their services, products and solutions and purchase them.



Since Cisco's solutions are different and vast, we are going to cover more on their SaaS, since doing so would help us cover every single component in their services being: hardware, software, network, cloud, security. This helps us cover as much as we can within the capabilities of university students.

Technical DFD

After exhaustive research and with the help of chatgpt, searching for what the main components of a SaaS would be and what would be the data transmitted between every process, this is the technical DFD conclusion reached.



While Cisco's solution for database management system products contain internal databases for their functionality, they are generally management systems for security infrastructure, not general-purpose database management systems providers. Which means aside from having a few internal databases embedded in systems like Cisco ISE and Cisco IOS XE, they rely on using oracle and microsoft to offer their DBMS platforms.

Identifying the possible impact of each component

For the business DFD model, each data store stores highly sensitive information such as “User credentials” and “payment credentials” and operational sensitive information such as “Product/Service Data”. All of this is on the website security from Cisco’s side to protect these information. If the User credentials data store was unavailable for 24 hours, it would cause huge operational damage and halt operations causing Cisco financial impact, the real issue would be if the User credentials and Payment credentials data stores were breached, as this would cause critical damage to Cisco’s financial state, loss of reputation as they are one of the world’s leading network organization and since Cisco is PCI DSS certified, this would mean there would hefty fines, expensive forensics investigation costs, potentially losing their certification and if the event was handled poorly, could cause the responsible member to be under liability of imprisonment. A leak in the Products and Service database would also cause incredible damage since the internal infrastructures of various organizations would be public, potentially leading organizations to raise legal issues and lawsuits on Cisco. This could also cascade into problems and attacks within the technical architecture DFD and this would lead to several threats and risk to be addressed. A breach like this could lead the attacker to know the components of an organization or their victim so then they can start building an attack vector for the victim and since Cisco has many partnerships and is well known for their software and hardware products, an attacker could get their hands on the operations and data of their victim.

From a technical architecture perspective, an attack on any of the data stores is devastating, as these attacks would leak a company's valued asset and information, give escalated privilege in various functionalities, allow for tampering with configurations and data and potentially even remove any sort of evidence of such an attack. This is both devastating for the victim and Cisco as Cisco will also be held liable for such attacks.

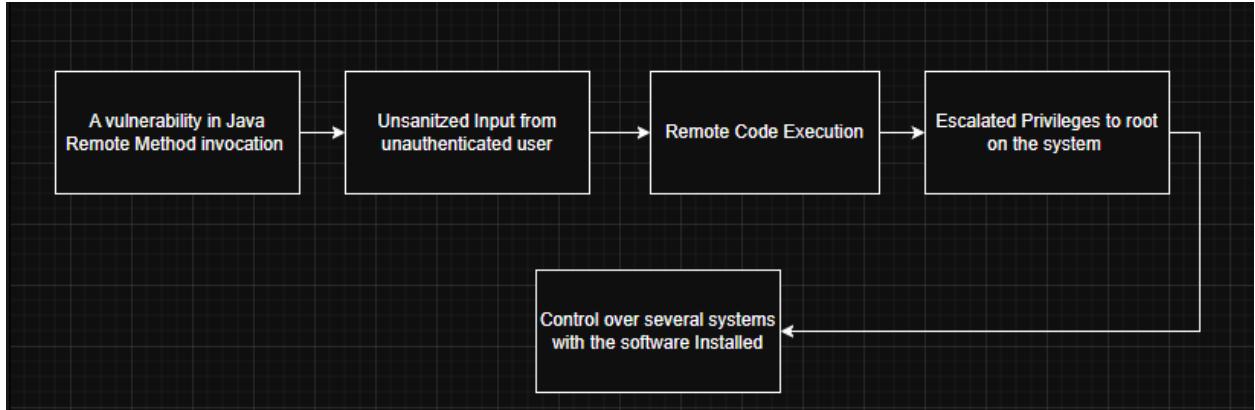
Advanced STRIDE Analysis with Attack Chain Modeling

Our first step to identify various threats that any of the processes above could face. There are numerous types of threats and we will address some of them and what the attack chain is or could have possibly been, including a threat propagation matrix showing how each threat can cascade through Cisco's system architecture.

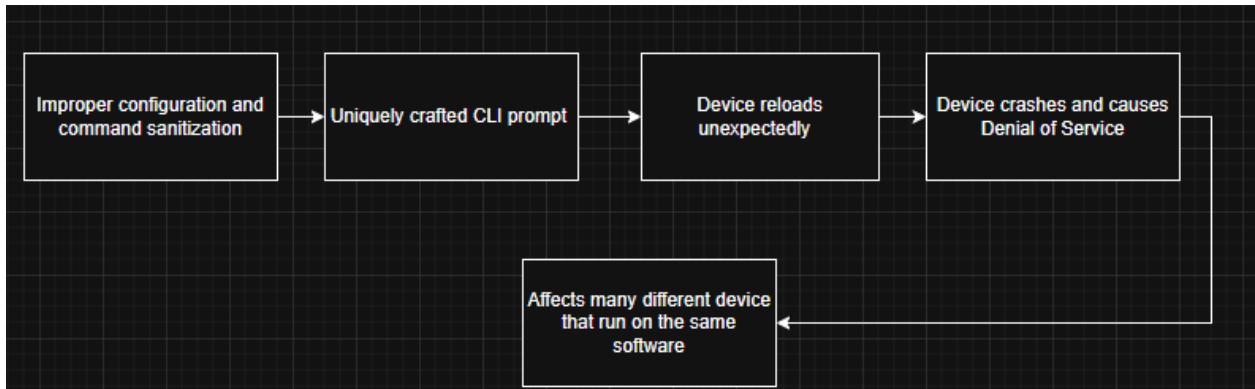
Propagation	1					
Impact/Likelihood	1 (Insignificant)	2 (Light)	3 (Damaging)	4 (Severe)	5 (Catastrophic)	
5 (Numerous)	5	10	15	20	25	
4 (Frequent)	4	8	12	16	20	
3 (Common)	3	6	9	12	15	
2 (Uncommon)	2	4	6	8	10	
1 (rarely)	1	2	3	4	5	

Above, this is the threat propagation matrix, where we can scale our threat based on 2 things, how common is it for the threat to propagate to other systems and how impactful is the threat on other systems. This helps us evaluate the context and value of our asset as well.

A remote code execution (considered as one of the most dangerous and critical threats) performed on one of Cisco's software where an unauthenticated, remote attacker uploads files and executes commands on a system with the software that can give the attacker escalated privilege to admin or root. On the STRIDE model, this would be classified as "Tampering" as the user was able to upload files and execute commands. Threat propagation rating would be 20 - (4 in likelihood and 5 in Impact) since having root privilege over a system would mean being highly likely to access other devices and softwares in the system depending on the trust boundary.

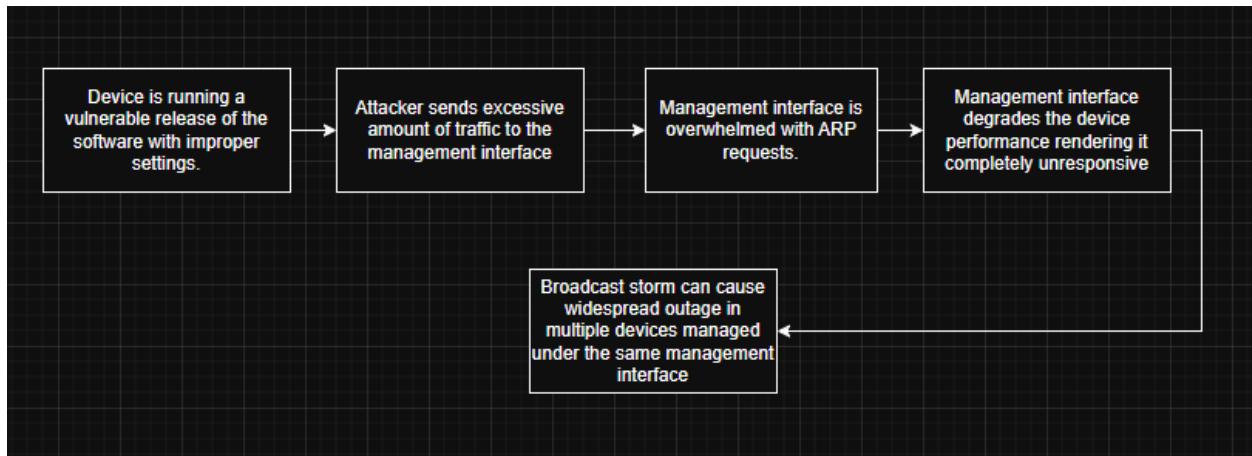


Lets search for a detailed possible vulnerability that could possibly affect Cisco network trafficking. We have learnt that one of the services Cisco provides is their computer network OS IOS. Most OS use Command Line Interface (CLI), and IOS does use CLI, so in this case, let's talk about what possible vulnerabilities their IOS CLI system might have.



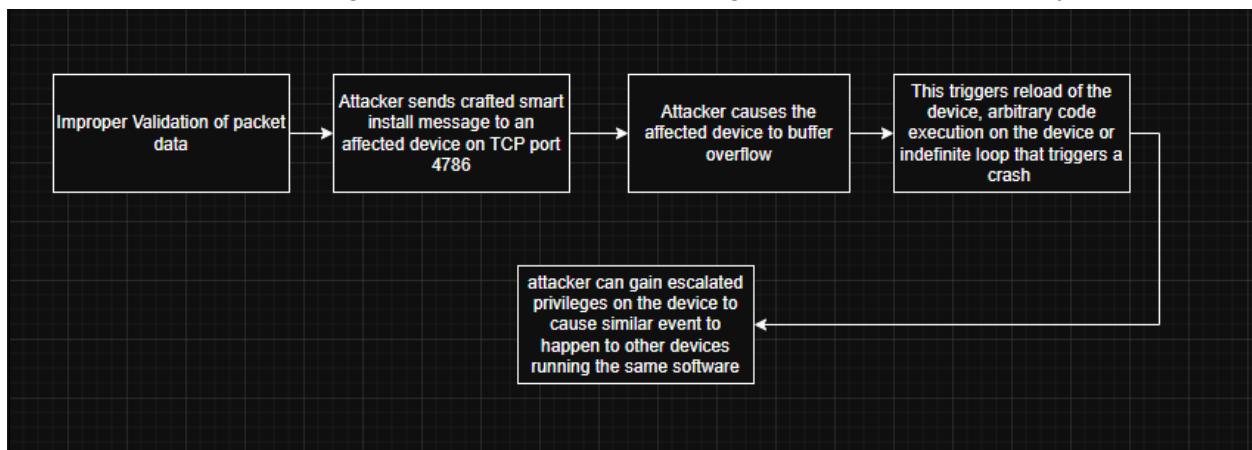
In this attack chain scenario, The attacker is a low privileged account that is able to access the CLI prompt on the Cisco IOS machine. The attacker is then able to craft a unique CLI command that causes the device to reload in an unusual manner which triggers denial of service. Although not dangerous, this threat unfortunately impacts a lot of the products that run the same Cisco IOS network. Under the STRIDE model, this would be a Denial of Service threat. Threat propagation would be 12 - (4 for Likelihood, 3 for Impact). The likelihood is self explanatory, the impact is 3 because this unexpected reload can cause other devices connected to the IOS to do so as well.

Since Broadcast storm is a fairly common attack within the DDOS scene, it's also safe to assume that Cisco could also risk having a broadcast storm attack performed on the same software they provide being the IOS and the NX product line.



In this attack chain scenario, a low privileged attacker can exploit a vulnerability in the ARP (address resolution protocol) implementation which could allow an unauthenticated, adjacent attacker to trigger a broadcast storm. This broadcast storm would fill the network traffic with broadcast requests to all devices, which would lead to unresponsiveness from many devices connected to this broadcast network. Under the STRIDE model, this would be Denial of Service. Threat propagation rating would be 15 - (5 for likelihood, 3 for impact).

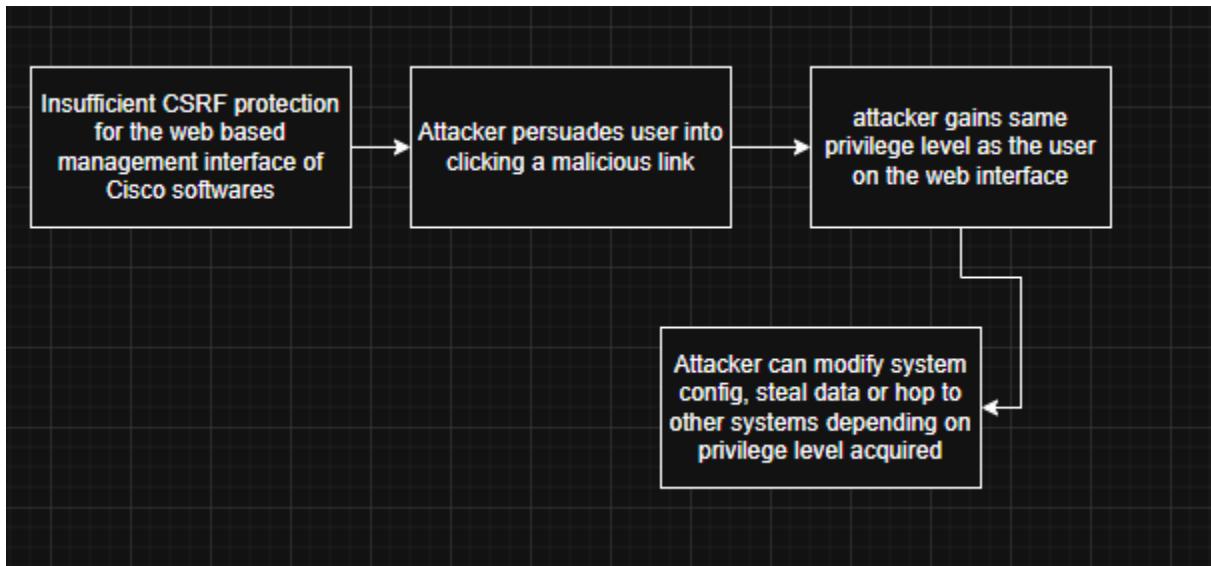
For this attack, we in fact went and checked Cisco's attack history to find an attack that was extremely dangerous for their systems and could impact Cisco financially as much as possible. Cisco released a document on one of their features that helps simplify deployment configuration called "[Smart Install](#)" Though its purpose is to make things easier, it raises security concerns.



In this attack chain scenario, The attacker is remote and unauthenticated on the device running this software. The Smart install feature in the Cisco IOS and Cisco IOS XE software could allow the attacker to trigger a reload on the affected device, causing Denial of Service or Remote code Execution. Under the STRIDE model, this can be classified under both "Tampering" and "Denial of Service". The Threat propagation rating would be 25 (5 for likelihood, 5 for impact). An attack like this is devastating, easily propagating to other systems if those systems are

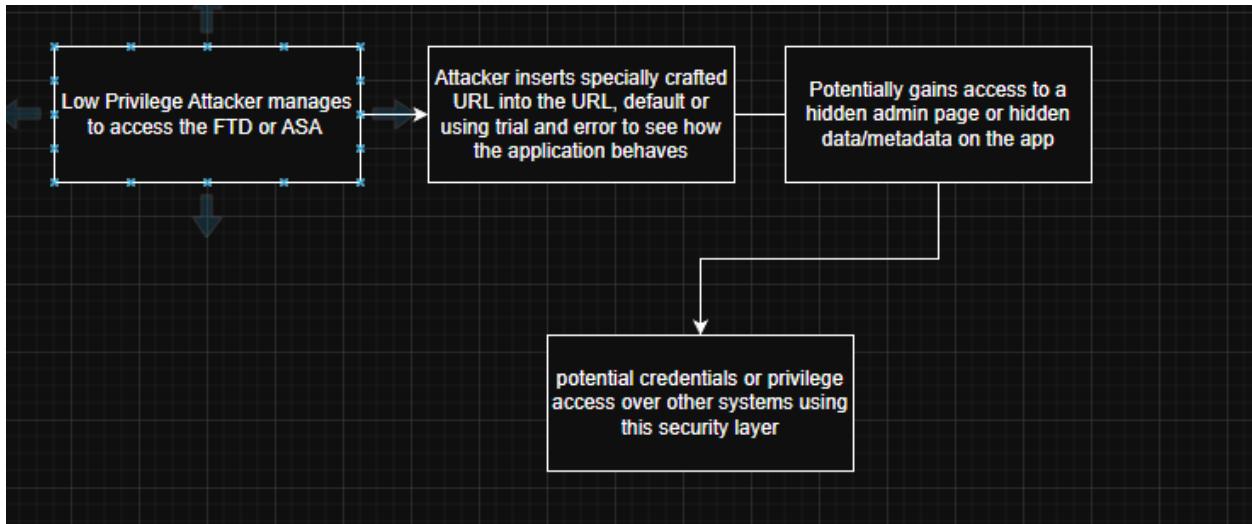
connected to the same IOS running and most definitely anything done on that device will be relayed to all the other systems.

For this one, we have decided to use another one of Cisco's software services to help increase the surface we are evaluating for any potential risks. This software is their Cisco Unified Communications Manager (CUCM). This software helps ease communications and session management unifies voice, video, messaging, and collaboration for businesses. Based on this, we could try to craft a scenario that might occur in a situation where our user has to be present for the attack to occur. Interesting find, that software uses CSRF tokens.



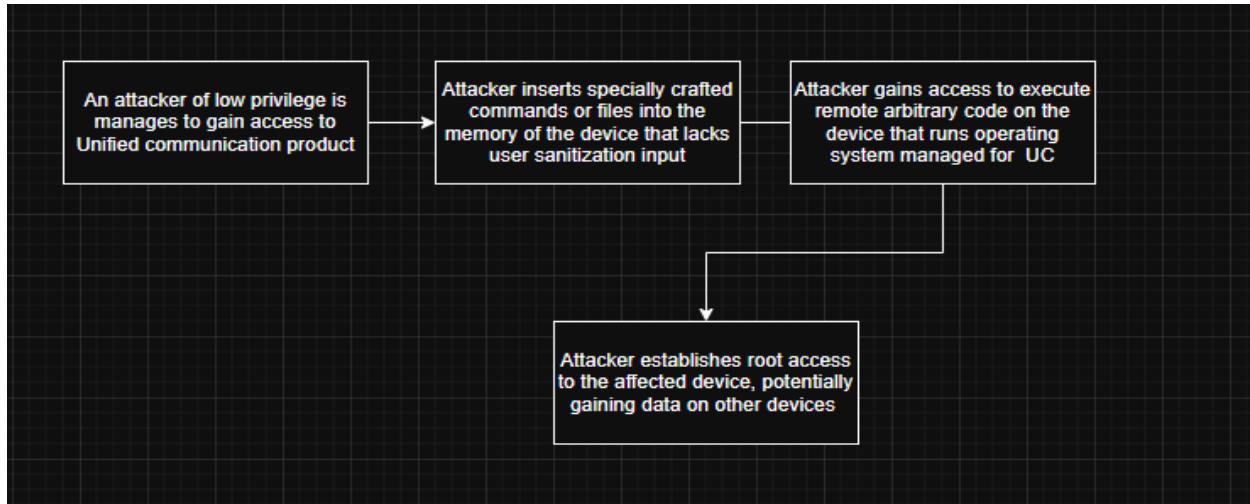
In this attack chain scenario, The attacker is remote and unauthenticated. The attacker persuades a user of Cisco Unified Communications Manager (Unified CM) Software or Cisco Unified CM Session Management Edition (SME) Software to click on a malicious link, which then the web interface doesn't properly validate the anti-CSRF token and causes the attacker to gain the same level of privilege as the user. Under the Stride Model, this can be classified under "Escalation of Privilege". In the Threat propagation rating, this would be 15 (3 for likelihood, 5 for impact) Escalation of Privilege could lead our attacker to gain unprecedented power over the current leading our attacker to know information about other systems through chats but it is also possibly unlikely.

So far we have spoken about software applications for Cisco such as the IOS and CUCM, let's talk about a possible vulnerability that could occur in the security layer of their operations. In particular, let's talk about Cisco's Adaptive Security Appliance (ASA) and Cisco's Firewall Threat Defense (FTD). Interestingly enough, both of these security applications have URLs for management.



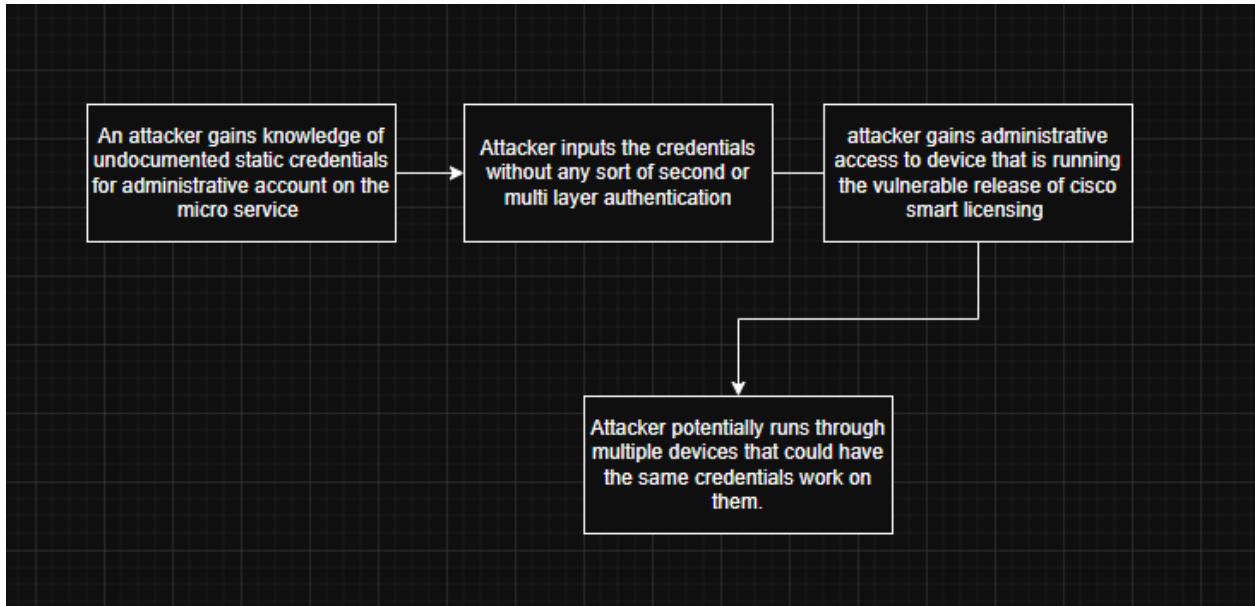
In this attack chain scenario, The attacker manages to gain access to the security application page, whether low or high privilege (it doesn't matter) they then craft special URLs to gain access to pages they are not authenticated to access. In the STRIDE model, this would be "Tampering" In the threat propagation matrix, this would be score 16 (4 for Impact, 4 for likelihood) Since no matter what, the impact on other, whether it be privilege escalation or data tampering or information disclosure, it would be impactful as well as the probability of gaining credentials to other systems is also high.

Heading back to Cisco's Unified communications products, Since this product line runs on a specialized Operating system and working on the current Linux distribution [AlmaLinux](#). We could say there is also potential for remote code execution.



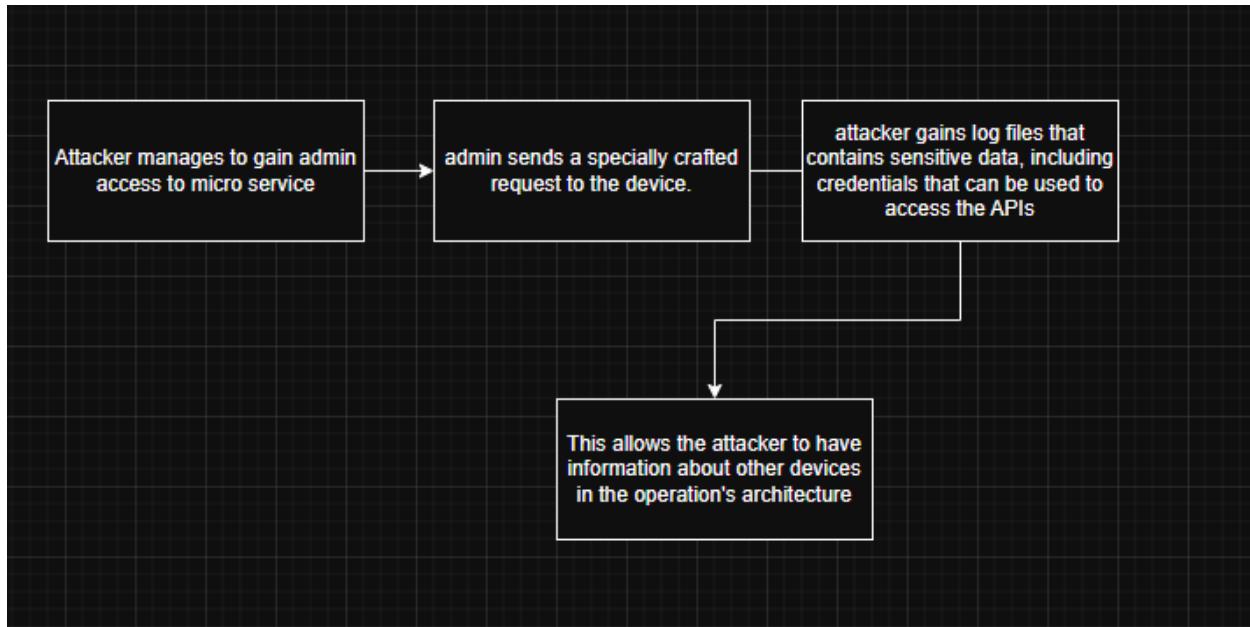
In this attack chain scenario, The attacker is potentially a low privilege user on the device running the operating system made to manage unified communications products to which they can enter data into the memory since there is a lack of input sanitization from the user, leading them to execute remote code on the device and giving them root access and privilege device. In the STRIDE Model this would be considered “Tampering” with a threat propagation score of 25 (5 for likelihood and 5 for impact) since there is a large product line that uses this operating system made for Unified Communication and like this that gives root access, this deserves a critical score.

We have now spoken so far about the security layer that Cisco provides as well as their softwares being the IOS and Unified communications, Though this one is a software, it also taps in a little of cloud and cloud services. A micro service that Cisco provides called “[Smart Licensing Utility](#)” which acts as a local proxy for devices that are not able to connect to the internet to use cloud services and collects data from multiple devices to give a smart report and feedback. Let us see a possibility of a misconfiguration that every network and device provider potentially makes



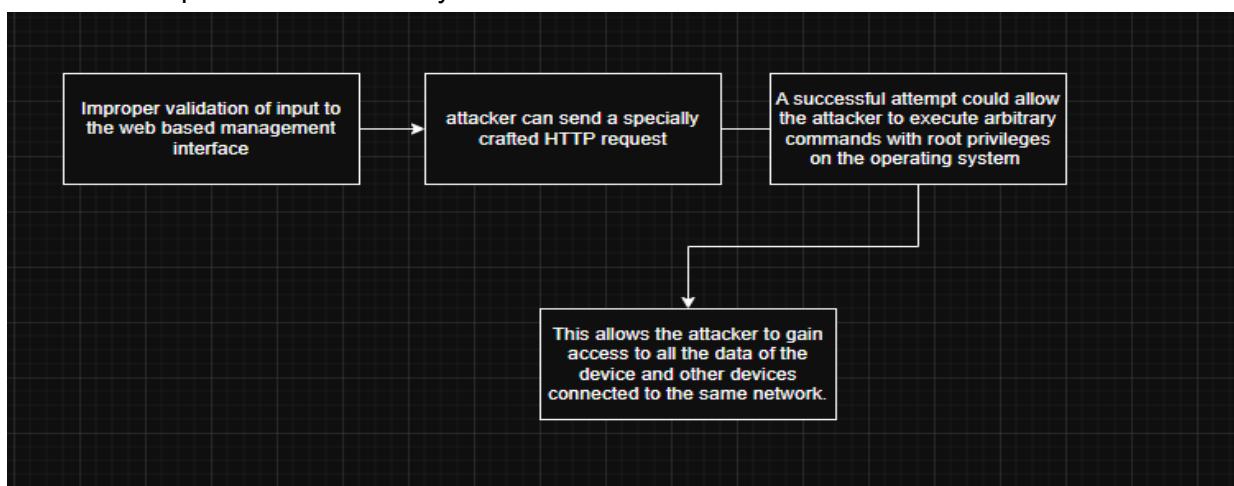
In this attack chain scenario, The attacker is able to get their hands on a undocumented static credentials for the administrative account for the smart licensing utility, giving them admin access to the device they are using or even potentially multiple devices that are running on the same licensing utility. In the STRIDE model, this would be classified as “Spoofing” with a score of 20 in the threat propagation (5 for likelihood and 4 for impact) since the attacker most definitely gains access to sensitive information collected from multiple devices and since the data is given to an administrator, the data is sensitive and could heavily impact the device and operations running with this micro service.

We could even build upon the vulnerability above, seeing that our attacker managed to use static admin credentials means they gain admin access to the smart licensing utility that then allows them to collect sensitive information they are not allowed to access.



In this attack chain scenario, The attacker already has admin privileges on the device and can send a specially crafted request to the device to gain sensitive information and credentials to access the APIs. This is built on the vulnerability that we found prior to this. In the STRIDE Model, this is classified as “Information Disclosure” and gets a threat propagation score of 9 (3 for Impact and 3 for likelihood) Sensitive information potentially could leak credentials to other devices and also potentially leak admin credentials, though it is not a given.

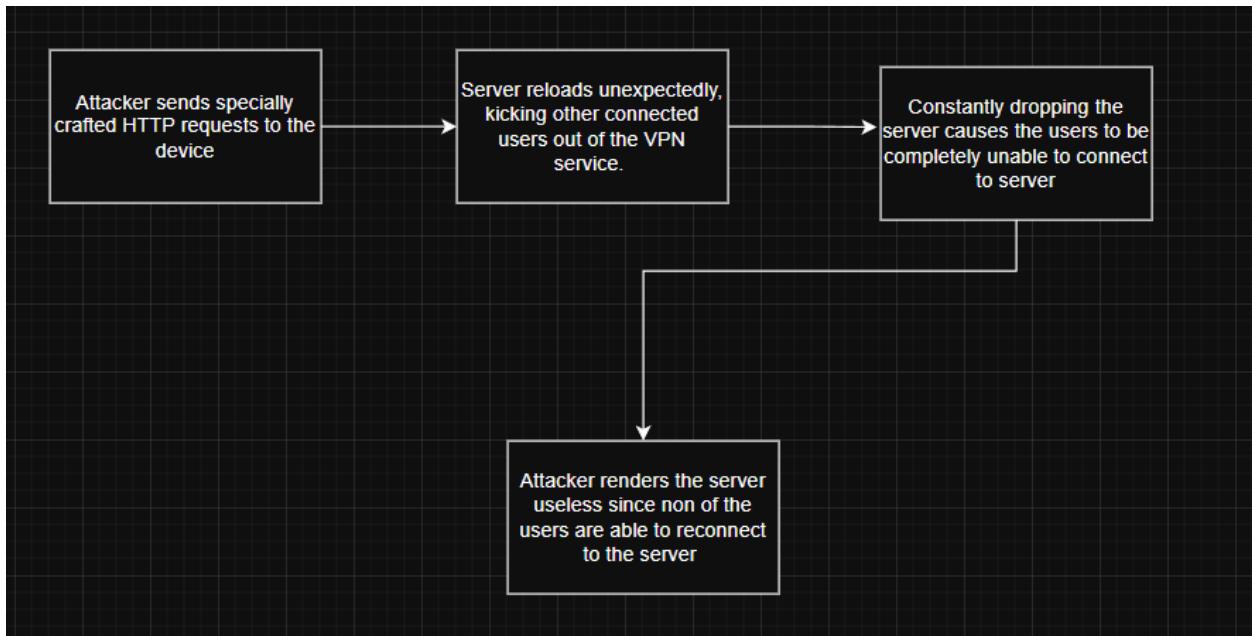
Another potential vulnerability finding in another of Cisco software applications named Cisco [“Unified Industrial Wireless Software”](#), this is a software that helps provide reliable and fast wireless connectivity in an industrial context where there could be heavy traffic and constant traffic flow in the network. Since they have a web based management interface that uses HTTP, let's look at a possible vulnerability that could occur.



In this attack chain scenario, The attacker manages to gain a low privilege access to the device, then because of the improper validation of user input, the user manages to craft a unique HTTP request to the device which then allows the attacker to execute arbitrary commands that gives

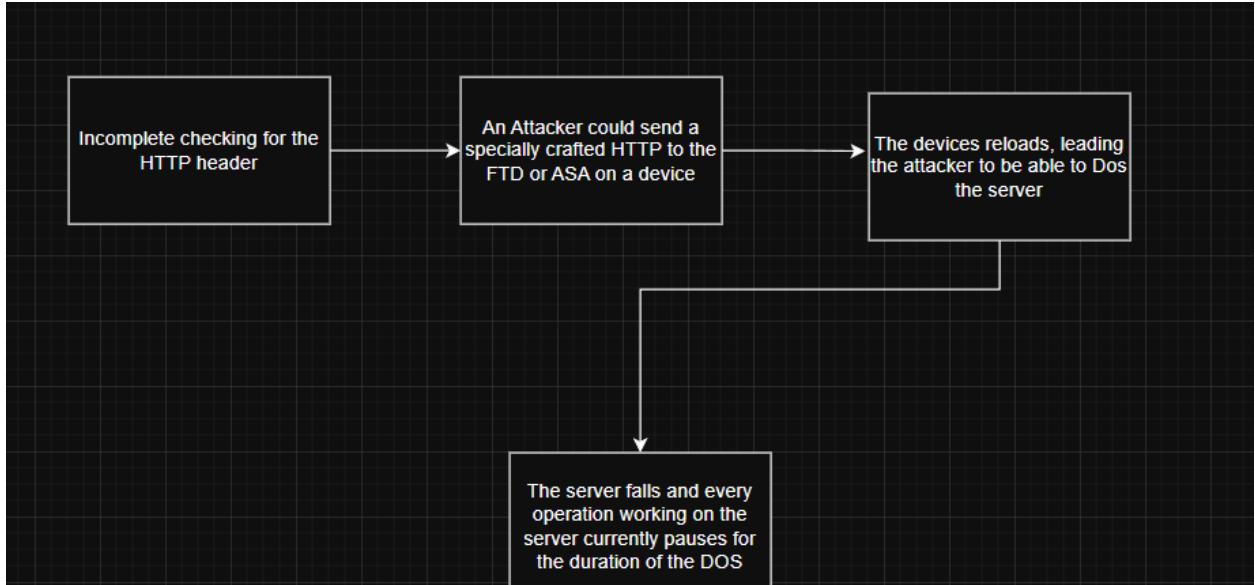
them root privileges, controlling over the entire device remotely. In the STRIDE Model, this would be classified under “Tampering” and would be rated 10 for threat propagation (5 for Impact, 2 for likelihood) Root privileges explains the 5 rating, but the reason why the likelihood of this propagating to other devices is because the product line for this vulnerability is very small, only 5 devices are affected by this vulnerability.

Let's touch on one of Cisco's biggest cloud market driver: Meraki. It's a cloud-managed IT platform that makes the management of Wi-Fi, security, switching and IoT devices by offering a single web based dashboard. Lets see what an attack possibility is with this especially including the “[AnyConnect](#)” VPN services which allows users from any place as if they were present in that network, it also provides endpoint security.



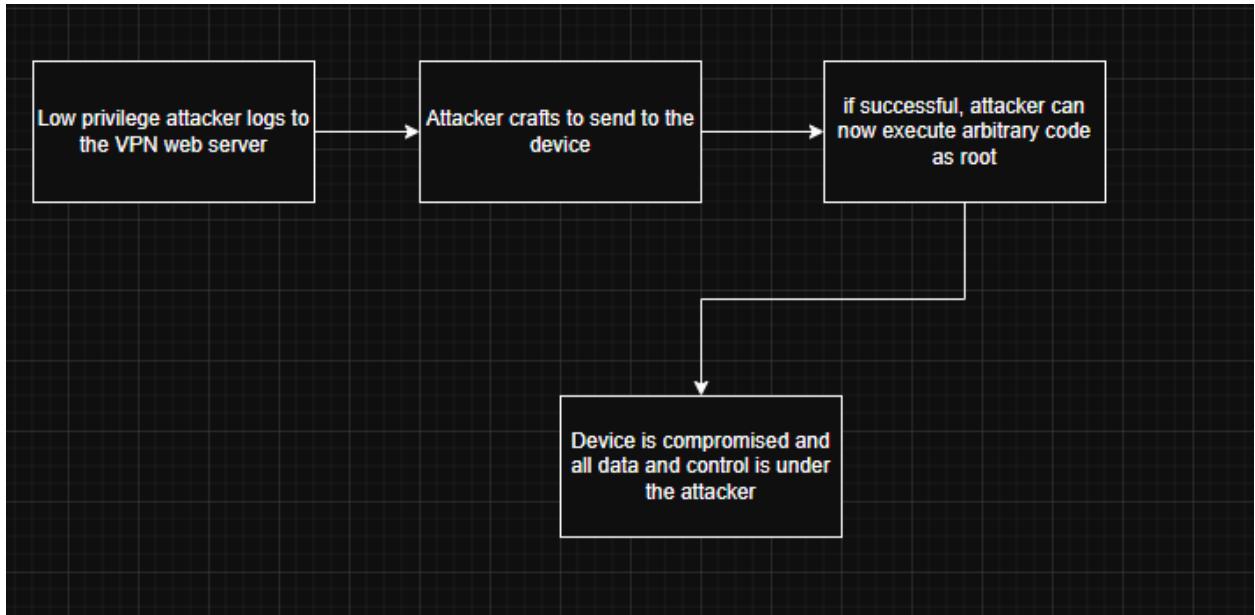
In this attack chain scenario, The attacker is unauthenticated but manages to craft a special HTTP request to the device, which causes the VPN server to restart, kicking all the users out of the network. With consistent attack, the attacker could render that vpn server useless so nobody is able to connect to it at all. In the STRIDE Model, this would be considered “Denial of Service”. Threat propagation would be 20 (5 for likelihood and 4 for impact) Since an attack like definitely disrupts other devices connected to the vpn and causes their network to be disconnected, stopping operations.

For the next vulnerability, it also includes the FTD and ASA security layer we spoke about earlier. Where an issue can arise in the management and web servers of both services.



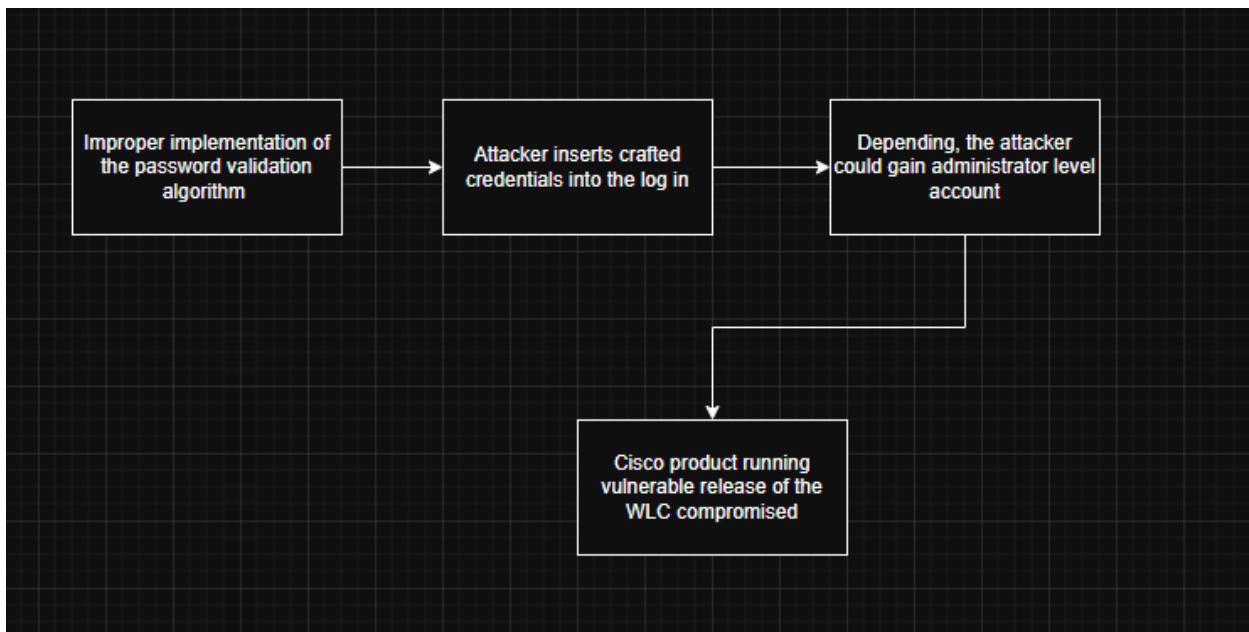
In this attack chain scenario, The attacker is unauthenticated and remote to cause the device to reload unexpectedly, resulting in DoS. This is due to incomplete checking on the HTTP header that leads our attacker to send a special HTTP request to the targeted web server on the device. If successful, this leads to a DoS attack. In the STRIDE Model this would be “Denial of service” and threat propagation score would be 6 (3 for impact and 2 for likelihood) this attack would only affect the current device and most probably won’t propagate to other device, but if it does, the DoS attack can be quite impactful on other systems.

Going back to the security layer which includes ASA and FTD, a scenario where the VPN web portal used daily by authenticated users to reach the network contains a flaw in how it handles HTTPS requests.



In this attack chain scenario, our attacker manages to log in to the device with valid user credentials to send crafted HTTP requests to the device. If successful, the user gains root access control on the device through remote code execution and compromises the device. In the STRIDE Model, this would be classified as “Escalation of Privilege” and would earn a threat propagation scoring of 20 (4 for likelihood and 5 for impact) since any device running the vulnerable release of FTD or ASA is under danger to be accessed to with root privileges.

After researching a little about Cisco Wireless LAN Controller (WLC), we found that it might be possible for an attack to occur on this software, a threat that was incredibly famous and was in the top 5 OWASP threats.



In this attack chain scenario, we are faced with an attack that roots from a commonly known attack named “SQL Injection”. Although it may not be a SQL Injection in itself, our attacker uses crafted credentials to try to crack into an account that they do not own. If successful, they could get control over an admin account, seizing admin access to the WLC device. In the STRIDE Model this would be classified as “Tampering” and could possibly be “Escalation of Privilege”. Threat propagation score would be 9 (3 for impact, 3 for likelihood) although getting admin privileges over the device is devastating and leads the attacker to know about other network endpoints, it is guaranteed this same threat can be reproduced on other devices that are not WLC related.

Risk Register and DREAD scoring based on the asset’s context.

For this part, we will create a risk register for every vulnerability we have mentioned above, most of these vulnerabilities are shown to be existing CVEs and do cause real damage to the systems we have researched and discussed about. We will be giving each risk its DREAD score

based on its current threat landscape, regulatory requirements (SOC, ISO 27001, PCI DSS, etc) in consideration of seasonal factors when attack frequency could increase or vary.

Before so, calculating Cisco's risk appetite for each asset is quite tricky to do with the threats we have measured, because Cisco does not publicly state a numeric "risk appetite" or a dollar amount they are willing to lose per product (IOS, ASA/FTD, cloud, microservices). Instead, Cisco expresses its risk appetite qualitatively, and in practice it is very low for security, availability, and trust, and moderate for innovation and revenue risk. These are not only products that will impact Cisco financially, but since these products are also sold to other companies and organizations, there is also a financial impact for these companies and it would be Cisco's fault partially. Loss of reputation, loss of trust from customers and potential lawsuits raised against them is also another thing to take into impact and how that would affect their face as a network vendor and their profits. We would know from all of this that their risk appetite for technically any product would be very low, since we also know that Cisco they perform out-of-cycle patches for Critical CVEs, Customers are strongly urged to upgrade, product lines are sometimes "end of life" early than to be left exposed.

Below is what a full Risk register would look like, taking in account for the Risk's Description including which CVE it correlates to and all the information we have gathered from the risk. Below every 5 risks registered, there will be DREAD score justification, carefully assessing each score given to each letter of the DREAD for each risk registered.

Risk Description	Regulatory Requirements	Impact Description	Impact Level	Probability Level	DREAD Scoring	Contextual DREAD Explanation	Mitigation Notes	Owner
CVE-2025-20354, Multiple vulnerabilities in the Java Remote Method Invocation allows file upload and remote code execution	ISO 27001 A.9 Access Control, A.13 Network Security Controls.	Potential Privilege Escalation to root on the system. Having access to all the info within system and other systems as well	5	2	Damage - 10 Reproducibility - 6 Exploitability - 4 Affected Users - 10 Discoverability - 2	Gaining root privileges is catastrophic. During a Company's peak season, can completely halt operations and affect all users within system	validate and restrict all uploaded content, tightly limit access to the RMI service	Lead Software engineer
CVE-2025-20419, Unsanitized input into the CLI command makes device reload unexpectedly leading to DOS	ISO 27001 A.8.28 - secure coding, A.8.19 - configuration management, SOC 2 CC6.6	Potential Buffer overflow, which triggers the device to reload and DOS, collapsing all network operators on the IOS, which is crucial to it	3	2	Damage - 5 Reproducibility - 8 Exploitability - 2 Affected Users - 4 Discoverability - 5	Dropping the service IOS provides could cause it to lose data and operations to malfunction. Only current data in traffic might be lost, bad during peak hours	based access controls with command authorization, sanitize and whitelist all CLI inputs, and enforce rate-limiting	Cisco Network Operating Systems Engineering Lead
CVE-2025-20340, misconfigured Address Resolution Protocol implementation can allow unauthenticated attacker to broadcast storm	ISO A.13.1.1 - Network security controls must prevent flooding attacks. ISO A.12.6.1 - vulnerability management	This would cause broadcast storm which would flood the network traffic and halts normal network traffic.	3	3	Damage - 3 Reproducibility - 8 Exploitability - 5 Affected Users - 8 Discoverability - 5	Crashing the network during peak hours could cause a lot of data to be lost during transmission. This would be operationally damaging.	Enable storm control, ARP rate-limiting, port security, and proper VLAN segmentation to prevent and contain ARP-induced broadcast storms.	Network Administrator
CVE-2018-0171, sending a crafted smart install message to the device on TCP port 4786, which might lead to a successful buffer overflow	ISO A.14.2.5 - Secure Development SOC 2 CC7.1 / CC7.2 - detect and mitigate exploitable flaws.	3 potential impacts occur from this attack: Triggering a reload of the device or execute arbitrary code on the device or watchdog crash	5	2	Damage - 10 Reproducibility - 9 Exploitability - 3 Affected Users - 10 Discoverability - 4	Any of the following impacts in any given context is devastating because it affects all IOS installed devices that has the smart install feature	secure update mechanisms to prevent uniquely crafted install-feature messages from triggering device reloads	Lead Software engineer
CVE-2025-20326, insufficient CSRF protections in the web management interface allow an unauthenticated attacker to trick an admin into clicking a malicious link	ISO A.8.28 / A.14.2.5 - secure application development must prevent known web vulnerabilities. SOC 2 CC6.x - access control protections.	The attacker can trick a user whether low privilege or admin into clicking a malicious link to receive their privileges over the software and data	4	4	Damage - 9/4 Reproducibility - 9 Exploitability - 8 Affected Users - 8 Discoverability - 7	If the attacker gains low privilege, the attack isn't as devastating as receiving admin perms. Since CSRF is well known, this can be a consistent attack throughout seasons	Implement anti-CSRF tokens correctly, enforce same-site cookies, validate request origins.	Web Application Security Engineer

Dread Scoring Justification

CVE-2025-20354

Damage – 10

- Successful exploitation gives *remote code execution* on the IOS system.
- Full privilege escalation means total compromise of device functions, routing, switching, logs, and configurations.
- Worst-case impact is catastrophic and leads to maximum score.

Reproducibility – 4

- Exploit is possible if the misconfiguration is present, and the method invocation interface is exposed.
- However, it typically requires the right timing and a correct RMI path, making it not “trivially repeatable.”
- High but not guaranteed, 4/10.

Exploitability – 4

- Requires:
 - Network reachability to the RMI service
 - Upload capability
 - Some protocol understanding
- Not trivial like a basic web exploit which means moderate difficulty.

Affected Users – 5

- A compromised IOS device affects the entire network segment behind it.
- The severity is high but confined to users of that switch/router = midpoint justified.

Discoverability – 2

- The vulnerable interface is often hidden unless one scans internal management ports.
- Attackers won't easily find it externally due to ACLs and segmentation.
- Low discoverability, 2.

CVE-2025-20419

Damage – 5

- Causes IOS reload or DoS, disrupting service but **not** compromising confidentiality or full system access.
- Medium damage, 5.

Reproducibility – 8

- Once the malformed command is known, it behaves consistently and crashes IOS almost every time.
- Near guarantee of reproduction = 8.

Exploitability – 5

- Requires some level of CLI access or an API path feeding into CLI logic.
- Not trivial but not highly restricted = mid-range.

Affected Users – 5

- A rebooted switch/router affects all users on affected interfaces.
- Network-wide ripple effect = moderate to high.

Discoverability – 10

- The vulnerable CLI path is extremely easy to find because:
 - CLI is a core interface
 - Any fuzzing or malformed input will reveal it
- Maximum score.

CVE-2025-20340

Damage – 3

- Attackers can poison ARP tables which means traffic redirection or disruption.
- Damage is harmful but not system-destroying, no privileged code execution.

Reproducibility – 8

- ARP poisoning tools are widely available.
- Works consistently if ARP protection mechanisms are disabled.

Exploitability – 3

- Requires network layer adjacency.
- Harder to perform remotely; depends on LAN positioning.

Affected Users – 7

- ARP poisoning disrupts multiple hosts, especially in shared VLANs.
- Can impact many users simultaneously.

Discoverability – 8

- Misconfiguration is easy to detect:
 - Lack of ARP inspection
 - Lack of port security
 - Simple network scan reveals ARP behavior
- High discoverability.

CVE-2018-0171

Damage – 10

- Smart Install RCE allows pushing arbitrary configuration or redirecting traffic.
- Complete takeover of device behavior meaning maximum impact.

Reproducibility – 7

- Exploit scripts are public and reliable.
- Works consistently as long as Smart Install is enabled.

Exploitability – 2

- Requires:
 - Access to TCP port 4786
 - Device using Smart Install (increasingly rare due to deprecation)
- Low overall exploitability due to decreasing prevalence.

Affected Users – 10

- A compromised switch affects the entire network behind it: massive user impact.

Discoverability – 2

- Hard to find unless scanning specifically for Smart Install.
- Many networks hide this behind ACLs which means low discoverability.

CVE-2023-2032

Damage – 9

- CSRF can force privileged admins to perform unintended actions:
 - Enabling features
 - Changing configuration
 - Creating users
 - Pivoting into further compromise
- Not full RCE, but near-maximum because admin actions equal system-level impact.

Reproducibility – 4

- Works reliably only if the target admin:
 - Is logged in
 - Clicks malicious link
- Social engineering variability = moderate reproducibility.

Exploitability – 10

- Very easy:
 - Anyone can embed a CSRF payload in a webpage
 - No authentication required by attacker
- Fully remote and trivial.

Affected Users – 8

- Only privileged accounts are directly affected, but their actions compromise the entire system.
- Network-wide secondary effects gives high score.

Discoverability – 7

- Lack of CSRF tokens is easily detectable through:
 - Browser dev tools
 - Proxy inspection
 - Basic security testing
- High but not trivial discoverability.

CVE-2024-20353 XSS in Cisco ASA WebVPN login page allows session hijacking	ISO 27001 A.14.2.5, SOC 2 CC7.1	Attacker steals admin session cookies, gains unauthorized access to VPN	4	3	Damage - 7 Reproducibility - 8 Exploitability - 6 Affected Users - 7 Discoverability - 5	Old vulnerability still exploited; can lead to full network access during peak hours	Patch ASA, implement Content Security Policy (CSP), use WAF	Network Security Team
CVE-2023-20198 Unauthenticated RCE in IOS XE Web UI allows full device takeover	ISO 27001 A.13.1.1, NIST CSF PR.AC-5	Attacker executes commands as root, controls switch/router	5	3	Damage - 10 Reproducibility - 9 Exploitability - 8 Affected Users - 10 Discoverability - 4	Actively exploited in attacks; can disrupt entire network segments	Disable Web UI if unused, apply patch, segment network	Network Engineering
CVE-2025-20352 – SNMP DoS in Cisco IOS/IOS XE lets attacker with SNMP credentials send packets that reload the device.	ISO 27001 A.12 (Operations security), SOC 2 CC4.1	Routers or switches can restart and stop forwarding traffic, so users lose access to internal systems and Internet services.	4	3	Damage - 7 Reproducibility - 8 Exploitability - 6 Affected Users - 7 Discoverability - 6	DoS on core routers can disrupt many users, but attacker must already have SNMP access	Disable SNMP where not needed, use strong/limited SNMP credentials, and apply Cisco patches for the SNMP vulnerability.	Network Administrator
CVE-2025-20333 (ASA / FTD WebVPN Remote Code Execution) A critical bug in the VPN web service on Cisco ASA and FTD lets an attacker send crafted HTTPS requests and run code as root on the firewall.	PCI DSS 1.1, 6.2 (secure perimeter and timely patching), SOC 2 CC7.1 (prevent unauthorized access).	If the firewall is taken over, the attacker can turn off rules, read or change traffic, and move into internal networks.	5	4	Damage - 10 Reproducibility - 8 Exploitability - 9 Affected Users - 9 Discoverability - 7	Internet-facing firewalls with this bug can be fully taken over by remote attackers.	Patch ASA/FTD to the fixed version, disable unnecessary web VPN features, and restrict management/VPN access to trusted IPs only.	Firewall / Perimeter Security Engineer
CVE-2022-20695 (Wireless LAN Controller Authentication Bypass) A flaw in Cisco Wireless LAN Controller (WLC) software allows a remote attacker to log in to the management interface without a valid password in certain configurations.	ISO 27001 A.9 (access control), NIST 800-53 AC-2 (account management).	The attacker can manage wireless networks, change SSIDs, push new configurations and possibly capture or redirect Wi-Fi traffic.	4	2	Damage - 8 Reproducibility - 7 Exploitability - 7 Affected Users - 6 Discoverability - 5	An attacker could silently take over the wireless network, redirect traffic, and capture sensitive data without needing a password—especially risky in large offices with unmonitored Wi-Fi.	Check WLC configuration against Cisco's advisory, remove the vulnerable setting, and upgrade to the fixed software version.	Wireless Network Engineer

Dread Scoring Justification

CVE-2024-20353

Damage – 4

- XSS steals admin/user cookies which leads to unauthorized VPN access.
- Serious but does **not** grant device-level compromise or RCE.
- Medium damage.

Reproducibility – 3

- Works only if:
 - The vulnerable login page is exposed
 - The victim user interacts with the malicious payload
- Not consistently reproducible against all users.

Exploitability – 4

- Requires injecting crafted JavaScript into a vulnerable parameter.
 XSS methodology is common but requires finding the exact vulnerable field.

Affected Users – 7

- If a VPN admin/session token is compromised:
 - Multiple users indirectly affected
 - VPN access can be stolen + pivot into internal networks
- High user/system impact.

Discoverability – 3

- The vulnerable parameter is not obvious.
- Requires manual testing or automated XSS fuzzing

CVE-2023-20198

Damage – 10

- Full RCE as root means complete takeover of router or switch.
Maximum possible damage.

Reproducibility – 9

- Fully reproducible once the crafted payload is known.
- Exploits were mass used in the wild (as noted).

Exploitability – 10

- No authentication required.
- HTTP(S) request alone are extremely easy.

Affected Users – 5

- The compromised device affects its entire connected environment.
- But the effect still depends on the device's role midpoint justified.

Discoverability – 4

- The vulnerable web UI path is “discoverable” but not trivial.
- Attackers often scanned for it, but it's not exposed in all networks.

CVE-2025-20352

Damage – 3

- DoS causes router reloads = temporary outage.
- No data loss, no RCE, no privilege escalation.

Reproducibility – 8

- SNMP-based DoS works consistently once triggered.
- Certain message types cause predictable crashes.

Exploitability – 6

- Requires SNMP access + crafted packets.
- SNMP often limited to internal networks which means this is somewhat restricted.

Affected Users – 7

- Router reload affects:
 - Several upstream users
 - Routing tables
 - Branch networks
- High but not catastrophic.

Discoverability – 6

- SNMP versions, communities, and open ports are easy to detect with scanning.
- But the specific crash condition requires more testing.

CVE-2025-20333

Damage – 10

- RCE as root on a firewall = total compromise.
- Firewall can be turned off, bypassed, reconfigured, or used as pivot into internal network.

Reproducibility – 9

- Once the attacker crafts the right HTTP/S payload with valid VPN credentials, the behavior is consistent.
- Recent attack variant reliably forces reloads (DoS).

Exploitability – 9

- Requires only valid VPN credentials + malicious HTTPS request.
- VPN credentials are common targets = low barrier.

Affected Users – 9

- If the firewall is taken over:
 - All downstream traffic and users are exposed
 - Network segmentation collapses
 - VPN access is at risk
- Very high impact.

Discoverability – 7

- WebVPN interface is usually exposed externally.
Vulnerable parameters are not obvious but HTTP traffic is easy to analyze.
- Moderately high discoverability.

CVE-2022-20695

Damage – 4

- Attackers can control SSIDs, redirect traffic, or modify wireless behavior.
- Serious but not equivalent to full infrastructure compromise.

Reproducibility – 8

- Works consistently once the bypass condition is met.
- Highly predictable exploit behavior.

Exploitability – 7

- Requires access to the WLC management interface.
- If the interface is reachable, the exploit is straightforward.

Affected Users – 6

- Wireless environments may contain large user bases.

- Many clients affected, but core wired network impact is limited.

Discoverability – 5

- Requires checking the WLC's authentication logic and configuration.
- Moderate difficulty; not trivial but not obscure.

13	CVE-2025-20362 Privilege escalation in Cisco ASA and FTD management interface allows a logged-in low-privilege user to gain admin rights on the device.	ISO 27001 A.9 (access control), SOC 2 CC6.2 (least privilege).	A help-desk or read-only account could become full admin and change firewall rules, VPN settings, or disable logging without approval.	4	3	Damage - 8 Reproducibility - 8 Exploitability - 7 Affected Users - 7 Discoverability - 6	Abuse of this bug turns any compromised low-privilege account into an admin on a critical edge device, but the attacker still needs some level of access first.	Patch ASA/FTD, review and limit local user accounts, enforce MFA and strong passwords for all firewall admins.	Firewall / Perimeter Security Engineer
14	CVE-2024-20253 Remote Code Execution in Cisco Unified Communications products allows an unauthenticated remote attacker to execute arbitrary code with high privileges.	ISO 27001 A.12.6.1 (technical vulnerability management), SOC 2 CC7.1 (prevent unauthorized access).	The attacker can fully take over the Unified Communications server, listen to calls, read messages, and pivot to other internal systems.	5	3	Damage - 10 Reproducibility - 8 Exploitability - 9 Affected Users - 9 Discoverability - 7	This is a critical RCE on a core communication system; a single compromise can expose many users and sensitive conversations, though exploitation needs specific network access.	Apply Cisco's fixed software version for all affected Unified Communications products, restrict management access, and monitor call-server logs for abnormal admin actions.	Unified Communications / VoIP Administrator
15	CVE-2024-20439 undocumented static admin credential in Cisco Smart Licensing Utility allows an attacker to log in as an administrator.	ISO 27001 A.9.2 (user access management), NIST 800-53 IA-2 (identification and authentication).	Unauthorized administrative access to the Smart Licensing Utility, allowing full system control and potential misuse of licensing services.	4	4	Damage - 8 Reproducibility - 9 Exploitability - 7 Affected Users - 7 Discoverability - 6	Because the credential is hardcoded, once it is known it can be reused across many deployments, making exploitation easy and highly repeatable.	Upgrade Smart Licensing Utility to a version where the static account is removed, restrict access to the licensing portal, and monitor for unusual admin logins.	Licensing / Infrastructure Security Owner
16	CVE-2024-20440 information disclosure in Cisco Smart Licensing Utility debug logs allows an attacker to obtain credentials by requesting log files over HTTP.	ISO 27001 A.10 (cryptography & key protection), A.12.4 (logging and monitoring).	Exposed logs can contain usernames, passwords, tokens or API keys, which attackers can use to access the web UI or APIs with full privileges.	4	4	Damage - 8 Reproducibility - 8 Exploitability - 8 Affected Users - 7 Discoverability - 6	Attackers do not need to break crypto; they only need to download logs to get working credentials, turning a simple info-leak into full account compromise.	Patch to the fixed release, disable unnecessary debug logging, and rotate any credentials or tokens that may have been stored in logs.	Platform / Application Security Engineer
17	CVE-2024-20418 vulnerability in Cisco Unified Industrial Wireless Software for Ultra-Reliable Wireless Backhaul allows unauthenticated remote code execution.	ISO 27001 A.13 (network security), IEC 62443-3-3 (industrial control system security, where applicable).	An attacker can take full control of industrial wireless access points, disrupt backhaul links, and impact critical OT or industrial networks.	5	3	Damage - 10 Reproducibility - 8 Exploitability - 7 Affected Users - 8 Discoverability - 5	This is a CVSS 10 remote code execution on infrastructure often used in critical environments; attacks can cause both IT and OT outages even if exploitation needs some targeting.	Apply Cisco security updates for all affected industrial wireless devices, isolate these networks, and monitor for abnormal management or firmware-update activity.	OT / Industrial Network Engineer
18									

CVE-2025-20362

Damage – 8:

- Privilege escalation to admin/root enables firewall rule changes, credential access, and traffic interception → near-total security boundary failure.

Reproducibility – 8:

- Once exploit conditions are met, escalation can be reliably repeated across affected versions.

Exploitability – 7:

- Requires authenticated low-privilege access, but no physical access or complex chaining.

Affected Users – 7:

- Any organization running vulnerable ASA/FTD releases; firewalls are high-value shared infrastructure.

Discoverability – 6:

- Not obvious from UI, but discoverable via reverse engineering or diffing patched binaries.

CVE-2024-20253

Damage – 10:

- Full remote code execution on core communications servers → total system compromise.

Reproducibility – 8:

- Network-triggered vulnerability; repeatable once exploit is built.

Exploitability – 9:

- No authentication required; reachable over internal or exposed service ports.

Affected Users – 9:

- Impacts all users relying on voice, messaging, and call infrastructure.

Discoverability – 7:

- Service parsing flaws are commonly discovered through fuzzing and protocol analysis.

CVE-2024-20439

Damage – 8:

- Admin access allows license manipulation, service impersonation, and lateral movement.

Reproducibility – 9:

- Consistent exploitation once misconfiguration or vulnerable setup exists.

Exploitability – 7:

- Requires access to licensing service, but no advanced exploit chain.

Affected Users – 7:

- Organizations using on-prem Smart Licensing proxies.

Discoverability – 6:

- Misconfigurations and auth flaws are detectable via config review or API testing.
-

CVE-2024-20440

Damage – 8:

- Exposure of passwords/API keys enables downstream system compromise.

Reproducibility – 8:

- Credentials persist until rotated; exploitation is repeatable.

Exploitability – 8:

- Low complexity log access or API access is sufficient.

Affected Users – 7:

- All systems relying on stored credentials (network-wide trust issue).

Discoverability – 6:

- Logs and config files are common attacker targets but not always publicly visible.
-

CVE-2024-20418

Damage – 10:

- Remote code execution in OT networks = safety, production, and operational risk.

Reproducibility – 8:

- Reliable once the exploit path is known.

Exploitability – 7:

- Requires network access to industrial wireless controllers.

Affected Users – 8:

- Impacts entire industrial environments (SCADA, PLCs, sensors).

Discoverability – 5:

- OT protocols and firmware are harder to analyze and less exposed.

Phase 2: Intelligence-Driven Reconnaissance

Digital Assets:

Thankfully, Cisco has uploaded in their official documentation "[How Cisco IT Uses Its Own IT Technologies to Achieve Business Resilience](#)" what their internal IT deployment is and even their locations, what every network requires and what asset they use to solve that problem. One issue Cisco is particularly concerned with tackling is network resilience. Stability is a concern when Cisco's network traffic is incredibly large, spanning across 70 countries. Cisco must ensure that any sort of attack on any of their systems, being a device ,such as laptop or phones, routers, switches or even data center systems must either be able to prevent the attack or quickly recover from one without disrupting major operations for an extended period of time. Their network design, which is redundant architecture that automatically recovers or reroutes communications around failures, helps protect their network infrastructure from all possible disruptions. Key assets would be:

- Cisco IOS that has software features that support the resilience such as nonstop forwarding (NSF), Hot Standby Router Protocol (HSRP), and stateful switchover (SSO).
- Cisco Catalyst LAN switches with support for conditions such as cooling and the Power over Ethernet (PoE) features.
- Standardized network equipment configurations that are maintained centrally and audited daily at Cisco Network Operations Center (NOC). NOC monitors the entire Cisco

network 24 hours a day, which allows the rapid problem detection and resolution that minimizes impact on users and business activity.

- Cisco Catalyst 6500 switches help keep building in MAN (metropolitan-area networks) available even if individual switches fail.
- All Cisco offices are supported by an uninterruptible power supply (UPS) that provides electricity to all devices and systems for more than 2 hours if there has been an outage.
- Cisco's major application servers and storage systems are housed in a data center on the San Jose campus.
- All Cisco campuses have deployed Cisco Aironet wireless LAN access points, enabling employees to easily connect to the Cisco network in conference rooms, cafeterias, and other areas

Great, we've seen that Cisco does use these assets which means any attack on these devices would also affect them if their campuses were the ones to be attacked, Cisco has a lot of partnerships, supply chain and are connected to numerous companies, [Partnerbase](#) says that they are connected to 1375 partners with one of its largest being MySQL (which would make sense because Cisco outsources its own database management system to Oracle and MySQL).

Cisco also has an estimated number of employees to be around 86,200, a 4.65% decline from 2024 which was around 90,400.

Digital Footprint – Domain Overview ([cisco.com](#))

For Phase 2 we treat Cisco's public web ecosystem ([cisco.com](#) and key product domains) as the attack surface entry point.

Using Website Informer, the main corporate domain [cisco.com](#) was profiled to understand ownership, hosting and basic traffic characteristics.

- [cisco.com](#) is registered to Cisco Technology Inc. via MarkMonitor, first created in May 1987 and currently set to expire in May 2026, which shows it is a long-lived, stable corporate domain.
- The site is hosted on Akamai Technologies infrastructure, with an IP in the 23.192.0.0/11 Akamai range and a mix of Akamai name servers and Cisco's own DNS servers ([ns1.cisco.com](#), [ns2.cisco.com](#), [ns3.cisco.com](#)).
- Website Informer reports a global rank around 319 and roughly 774,500 daily visitors, indicating that [cisco.com](#) is a very high-traffic, business-critical asset.
- Website Informer also lists key subdomains such as [id.cisco.com](#) (*Identity*), [software.cisco.com](#) (*Downloads*), and [security.cisco.com](#), which represent critical entry points for authentication and software supply chain operations.

Whois
Identity for everyone

Domains Hosting Servers Email Security Whois Deals

Enter Domain or IP WHOIS

cisco.com

cisco.com

Website Informer
The richest source of website information

Home Browser Extension Emails

Cisco.com

cisco.com

About Website Updated: Dec 5, 2025

AI Infrastructure, Secure Networking, and Software Solutions - Cisco

Cisco is a worldwide technology leader powering an inclusive future for all. Learn more about our products, services, solutions, and innovations.

Trustworthy

Network Data View All

This website is hosted with Akamai Technologies, Inc., which reserves the following IP addresses for **cisco.com**: 23.62.168.118. Moreover, DNS used with this website include a28-64.akam.net, a3-64.akam.net, ns1.cisco.com, ns2.cisco.com, ns3.cisco.com. Subnet identifier ranges from 23.192.0.0 to 23.223.255.255. Classless Inter-Domain Routing (CIDR) is 23.192.0.0/11. ARIN net type is Direct Allocation.

319 Global Rank

774.5K Daily Visitors

4 days ago Last scanned

38 years Domain Age

Network
View All

Whois
View All

Domain & Keywords

ADDRESSING DETAILS

- Hosting Company
Akamai Technologies, Inc.
- IPs
[23.62.168.118](#)
- DNS
a28-64.akam.net
a3-64.akam.net
ns1.cisco.com
ns2.cisco.com
ns3.cisco.com
- Subdomains
[id.cisco.com](#), [cloudssso.cisco.com](#), [community.cisco.com](#), [software.cisco.com](#), [amp.cisco.com](#), [apps.cisco.com](#), [jobs.cisco.com](#), [cloudaps.cisco.com](#), [directory.cisco.com](#), [security.cisco.com](#)

IP DETAILS

- NetRange
23.192.0.0 - 23.223.255.255
- CIDR
23.192.0.0/11
- NetName
AKAMAI
- NetHandle
NET-23-192-0-0-1
- Parent
NET23 (NET-23-0-0-0-0)

OWNERSHIP

- Created
1987-05-14
- Expires
2026-05-15
- Owner
Domain Administrator (Cisco Technology Inc.)
- Registrar
MarkMonitor Inc.
- Owner Emails
infosec@CISCO.COM
- Associated Emails
dns-info@CISCO.COM, csg-network@cisco.com, ilepore@cisco.com, frazerp@cisco.com, csg-dnsadmin@cisco.com and 5 more

WHOIS INFORMATION

- Domain Name
cisco.com
- Registry Domain ID
4987030_DOMAIN_COM-VRSN
- Registrar WHOIS Server
whois.markmonitor.com
- Registrar URL
<http://www.markmonitor.com>
- Updated Date
2025-04-13T10:06:28+0000
- Creation Date

The registrar of cisco.com is MarkMonitor Inc. and the name expires on 2026-05-15. According to open source data, you can reach the owner at infosec@CISCO.COM but please make sure you have a good reason for unsolicited messages. Their country of residence is United States of America.

Field	Value (from Website Informer)
Domain	cisco.com
Registrar	MarkMonitor Inc.
Created	1987-05-14
Expires	2026-05-15
Hosting company	Akamai Technologies, Inc.
Example IP	23.62.168.118
CIDR / Range	23.192.0.0/11 (Akamai)
Name servers	a28-64.akam.net, a3-64.akam.net, ns1/2/3.cisco.com
Global rank	~319
Estimated daily visitors	~774.5K

Website Informer
The richest source of website information

Meraki.cisco.com
meraki.cisco.com

About Website Updated: Aug 12, 2025

Wi-Fi 6E | Network Security | Switches | Routers | Cisco Meraki

Cisco Meraki is the leader in cloud controlled Wi-Fi, routing, and security. Secure and scalable, learn how Cisco Meraki enterprise networks simply work.

Network Data

This website is hosted with Akamai Technologies, Inc., which reserves the following IP addresses for **meraki.cisco.com**: 23.212.248.140, 23.212.248.149. Moreover, DNS used with this website include ns1.cisco.com, ns2.cisco.com. Subnet identifier ranges from 23.192.0.0 to 23.223.255.255. Classless Inter-Domain Routing (CIDR) is 23.192.0.0/11. ARIN net type is Direct Allocation.

View All

8.4K Daily Visitors

4 months ago
Last scanned

No data Domain Age

No data Global Rank

Network View All

Whois

Domain & Keywords

ADDRESSING DETAILS

- Hosting Company [Akamai Technologies, Inc.](#)
- IPs [23.212.248.140](#), [23.212.248.149](#)
- DNS [ns1.cisco.com](#), [ns2.cisco.com](#)

IP DETAILS

- NetRange [23.192.0.0 - 23.223.255.255](#)
- CIDR [23.192.0.0/11](#)
- NetName AKAMAI
- NetHandle NET-23-192-0-0-1
- Parent NET23 (NET-23-0-0-0-0)
- NetType Direct Allocation
- OriginAS
- Organization [Akamai Technologies, Inc. \(AKAMAI\)](#)

At present, the WHOIS information for **meraki.cisco.com** is unfortunately not available. Due to various potential reasons such as privacy protections, data maintenance, or registrar restrictions, we are unable to provide specific details about **meraki.cisco.com**'s registration and ownership status at this time.

Field	Value (from Website Informer)
Domain	meraki.cisco.com
Registrar	Not available (subdomain of cisco.com)
Created	No data

Expires	No data
Hosting company	Akamai Technologies, Inc.
Example IPs	23.212.248.140, 23.212.248.149
CIDR / Range	23.192.0.0/11 (Akamai)
Name servers	ns1.cisco.com, ns2.cisco.com
Global rank	No data
Estimated daily visitors	~8.4K

Website Informer shows that `meraki.cisco.com` is also hosted on Akamai infrastructure and uses Cisco's own name servers, but traffic is lower (~8.4K daily visitors) and WHOIS details are hidden because it is a subdomain of `cisco.com`. This subdomain hosts the Cisco Meraki cloud-managed networking portal, making it an important part of the external attack surface for Wi-Fi, routing and security management.

Subdomain Enumeration (DNSDumpster)

DNSDumpster reveals many internal-sounding subdomains for `cisco.com`, including `dev`, `tst` (test), and `dr` (disaster-recovery) hosts, all in the Cisco ASN 109 address space. From an attacker's view, development and test environments are attractive because they often run older builds, weaker access controls, or extra debugging services. Mail (`*.mx.cisco.com`) and DNS (`ns1/2/3.cisco.com`) hosts are also strategic targets because they control email delivery and name resolution for the whole organization.

Showing 50 records out of a total of 95801 found.					
A Records (subdomains from dataset)					
Host	IP	ASN	ASN Name	Open Services (from DB)	RevI P
11i-amsdr-csm-01.cisco.com	64.102.120.196	ASN:109 64.102.0.0/16	CISCOSYSTEMS United States		1
11i-amsdr-csm-02.cisco.com	64.102.120.197	ASN:109 64.102.0.0/16	CISCOSYSTEMS United States		1
11i-dev.cisco.com	64.102.120.185	ASN:109 64.102.0.0/16	CISCOSYSTEMS United States		1
11i-dev-06.cisco.com	64.102.120.169	ASN:109 64.102.0.0/16	CISCOSYSTEMS United States		1
11i-dev-08.cisco.com	64.102.120.180	ASN:109 64.102.0.0/16	CISCOSYSTEMS United States		1
11i-dev-09.cisco.com	64.102.120.181	ASN:109 64.102.0.0/16	CISCOSYSTEMS United States		1
11i-dev-10.cisco.com	64.102.120.182	ASN:109	CISCOSYSTEMS		1

Subdomain	IP	Role / Environment (inferred)	Notes / Risk idea
11i-dev.cisco.com	64.102.120.185	Application dev server	Internal dev; if exposed, can leak code or configs. dnsdumpster
11i-dev-10.cisco.com	64.102.120.182	Dev node	Shows multiple dev hosts in same /16 range. dnsdumpster
11i-tst-03.cisco.com	64.102.120.137	Test environment	Test systems often weaker security controls. dnsdumpster
11i-dr-csm-01.cisco.com	64.102.120.245	Disaster-recovery / CSM node	DR infrastructure is also part of attack surface. dnsdumpster

11i-ssodev-nat.cisco.com	64.102.120.176	SSO development gateway	Dev SSO system could expose identity-related data. dnsdumpster
alln-mx-01.cisco.com	173.37.147.230	MX mail server	Mail infra targets for phishing / spoofing. dnsdumpster
rcdn-mx-01.cisco.com	72.163.7.166	MX mail server (regional)	Multiple MX hosts show globally distributed mail. dnsdumpster
ns1.cisco.com	72.163.5.201	Authoritative DNS	Critical for domain control and subdomain creation. dnsdumpster
ns2.cisco.com	64.102.255.44	Authoritative DNS	Located in Cisco ASN 109 address space. dnsdumpster

Subdomain Analysis: Meraki Cloud Portal

The DNSDumpster result for [meraki.cisco.com](#) shows it fronted by Akamai edge nodes in the 23.57.90.0/24 range, confirming that the Meraki cloud portal is delivered via a CDN. This means security of both Cisco's own backend and Akamai's edge configuration contribute to the overall attack surface

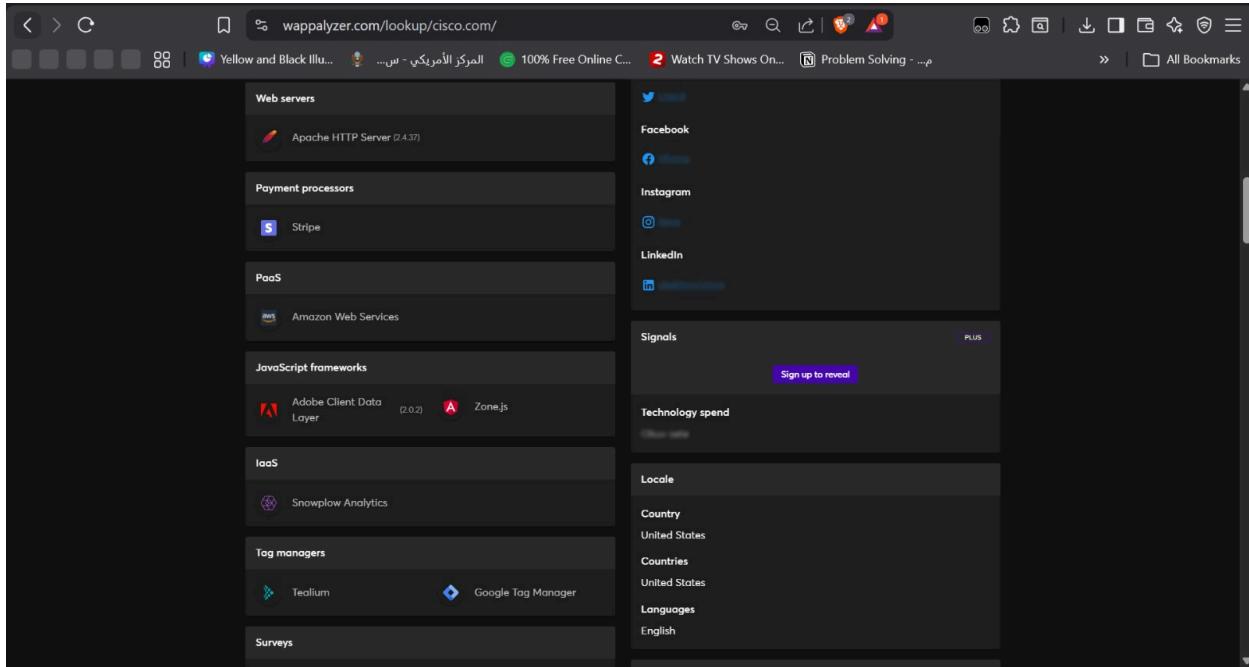
Subdomain	IPs	Provider / ASN	Notes
meraki.cisco.com	23.57.90.28, 23.57.90.31	Akamai (ASN 20940)	Front-end for Meraki cloud, load-balanced over Akamai edge. dnsdumpster

Having mapped the infrastructure, we next analyzed the software components running on the main corporate portal to identify potential application-layer vulnerabilities.

Technology Stack Fingerprinting (Wappalyzer)

Wappalyzer shows that cisco.com is a complex, marketing-heavy site built on Adobe Experience Manager and Apache HTTP Server, with Java and Python on the backend and delivered through Akamai and Amazon S3. The page uses many client-side frameworks and analytics/tagging tools (jQuery, Adobe Client Data Layer, Tealium, Google Tag Manager, Adobe Analytics, Google Analytics, AppDynamics, etc.), which increases the number of third-party scripts running in the browser. From an attacker's perspective, bugs in these web components (for example, vulnerabilities in AEM, JavaScript libraries, or misconfigured tags) could provide entry points into Cisco's customer-facing web applications.

Category	Example technologies detected on cisco.com
Web server	Apache HTTP Server 2.4.37
Programming languages	Java, Python
CMS	Adobe Experience Manager
CDN / hosting	Akamai, Amazon S3
Cloud / PaaS	Amazon Web Services
JavaScript frameworks	Adobe Client Data Layer, Zone.js
JS libraries	jQuery, Lodash, Underscore.js, core-js, Preact, jQuery UI
Analytics	Google Analytics (UA), Adobe Analytics, AppDynamics, Contentsquare, Mixpanel, Snowplow Analytics
Tag & data platforms	Google Tag Manager, Tealium, Adobe Audience Manager, Adobe Experience Platform Identity Service
Security features	HSTS, Akamai Bot Manager, reCAPTCHA
Personalisation / A/B	Adobe Target, 6sense, iGoDigital, Contentsquare
Payments	Stripe



Shadow IT/ Forgotten Assets

We've gathered some information on what Cisco's current infrastructure looks like, but we want to know if there is the possible "Shadow IT" or hidden assets in play behind the scenes. What if there is an asset that Cisco forgot about that is possible in use today? Making it a weak link behind an infrastructure so reinforced. Cisco has already addressed these kinds of issues, so we skimmed through their blogs to see what juice we could find on this topic.

A blog from Salt Security named "[Lessons from the Cisco Data Breach—The Importance of Comprehensive API Security](#)" by Eric Schwake talks about Cisco Data breach on 15 October 2024. Although the data breach didn't occur in extremely highly sensitive data assets, the tokens and other sensitive information were a dangerous find to be exposed into the outside world, leaking even source code which could all be used by hackers as a stepping stone. The source of this problem are the exposed API tokens were exposed in a public facing environment meaning attackers often use low-visibility, forgotten assets (public repos, storage, dev/test servers, APIs) as entry points.

Another blog from SC Media named "[Cisco ASA firewalls still under attack; CISA issues guidance for patch](#)" written by Steve Zurier talks about the two security flaws [CVE-2025-20362](#), a 6.5 privilege escalation bug, and [CVE-2025-20333](#), a 9.9 remote execution flaw were actively exploited well before CISA issued the directive in

September. A China-linked threat group called “Storm-1849” also known as ArcaneDoor was targeting Cisco’s ASA firewalls throughout October. This recent discovery mainly highlighted how often edge devices are forgotten about and not patched, leading to a hidden asset in many companies that use them - including Cisco.

SC media has also written a blog named “[Cisco warns of continued exploitation of 10-year-old ASA bug](#)” also written by Steve Zurier. This blog is a gold find because Cisco on Dec. 2 updated an advisory from March 18 about a 10-year-old vulnerability in the WebVPN login page of Cisco’s Adaptive Security Appliance (ASA) software that could let an unauthenticated remote attacker conduct a cross-site scripting attack. Though it is rated medium Severity by NIST (6.1 rating) This was a very old and exploitable bug that potentially put many companies and Cisco itself in a very vulnerable situation and the attacker could have been undetected the whole period.

People Intelligence & Employee Footprinting

Goal: Identify key personnel, technical skills, and potential social engineering targets to understand the human attack surface.

First thing we have done is perform a quick Maltego company stalker scan on Cisco, but we have proceeded cautiously since we do not want to trigger any kind of IDS as well as this is just a research project, I won’t be actively seeking information I shouldn’t get my hands on unless it is open for the public to see.

Key findings was 2 personnels, first being “RR Donnelly” a global provider of marketing, packaging, print, and supply chain solutions, which with further research happens to be one of Cisco’s customers, using their network products in their operations.

The RR Donnelly finding is quite intriguing because it would help attacks find another vector to attack from as attackers who already know that Cisco is extremely secure would struggle to find anything against it. All this would help attackers find common ground between the customer and vendor which is often:

- Vendor portals
- Shared ticketing systems
- VPN access (which is historically common)
- Email trust (possible less aggressive filtering)
- Whitelisted domains or IP ranges

The second key finding was a person called **Carolyn Calzia** who has worked at Cisco from Jan 2000 till Dec 2020 as a consultant. This is a person who has been around Cisco operations for more than 2 decades and proves to be a very valuable and key employee for Cisco.

Using LinkedIn OSINT, we identified key Cisco security and engineering personnel. Analyzing their public profiles reveals the specific technologies and security practices used internally, which helps attackers tailor phishing campaigns or infrastructure attacks.

Name	Public role / speciality	OSINT-derived risk
Ryan Fetterman	Security Researcher, SURGe by Cisco Foundation AI – focuses on AI-driven security research.	High-value target for spear-phishing to obtain threat intel or internal AI security tooling information.
Tricia "Trish" Wolff	Security Research Engineering Technical Leader – FIPS 140-3 crypto, switching & routing.	Detailed knowledge of crypto modules and router security; social engineering her could expose design details.
Thulasirajan Alagarsamy	Technical Lead – test automation & network engineering at Cisco.	Access to test environments and automation pipelines; compromise could enable supply-chain style attacks.
Lavanya D P	Cloud Engineer at Cisco (cloud infrastructure & services).	Likely access to AWS/Akamai configs; targeted vishing or cloud-phishing could lead to control-plane abuse.
Michael Anyaegbu	Network Consulting Engineer – CCIE, SDWAN, Software Defined Networking (7 years at Cisco).	Deep SDN/SDWAN expertise; compromise could reveal network topology and segmentation weaknesses.
Bob Scarbrough	Executive Consultant – AI Infrastructure & Hybrid Cloud (26 years at Cisco, data center SME).	Extensive knowledge of UCS, Nexus, ACI, Tetration; ideal target for APT reconnaissance on data center architecture.

<u>Karrthik V.</u>	Customer Success Manager – Network & Cybersecurity (21 years at Cisco, former Product Manager).	Long tenure means deep institutional knowledge; phishing could compromise customer relationships and CSM portal access.
<u>Abella-Evel Ammam</u>	Cybersecurity & Network Engineering Intern at Cisco.	Less experienced staff may be more susceptible to phishing or fake "mentor" requests from attackers.

Of all the people mentioned above, only one of them being "Ryan Fetterman" has a [public github repository](#) that is labeled "Security Researcher" which most probably does indicate it is him, including that he has done work for SURGe. There seems to be no public repo made by Ryan to which any leaked credentials can appear but he does link his [X account](#) where he does post mainly about cybersecurity work and a little bit about his own personal stuff which can aid in phishing messages/emails.

Attack Vector Analysis:

The transparency of these profiles allows an attacker to:

1. Draft targeted phishing emails (e.g., sending a fake "Terraform Config Update" email to the DevOps engineers).
2. Map internal tools (knowing they use Jenkins/AWS allows attackers to prepare specific exploits for those platforms).

Breach Data & Credential Exposure Analysis

To assess the vulnerability of Cisco's human attack surface, we performed breach database reconnaissance using Have I Been Pwned (HIBP) against email addresses associated with identified Cisco personnel. This analysis reveals critical credential exposure that significantly elevates the risk of account compromise through credential stuffing and targeted phishing.

Key Findings

The HIBP queries identified multiple Cisco employees whose email addresses (both personal and corporate) appear in publicly available breach datasets. Notably, Fred Fernandes (

fred@cisco.com

) has been exposed in 23 historical data breaches, and Gemma Sahagun (

gsahagun@cisco.com

) in 13 breaches. These are not isolated incidents—they represent a widespread pattern of compromised employee credentials that attackers can immediately weaponize.

Breach Exposure by Employee

LinkedIn Profile	Name	Email Address	Data Breaches	Risk Level & Implications
Raga Setty	Raga Setty	g.sudha.nse@gmail.com	Unconfirmed (personal email)	Medium – Personal email linked to a detailed technical profile (Palo Alto, F5, Python automation); password reuse could grant access to corporate infrastructure. Public contact info increases phishing risk.

<u>Daniel G. Shea</u>	Daniel G. Shea	danielgshea@gmail.com	7 data breaches	Medium – Although personal email, 7 breach exposures indicate repeated credential reuse pattern; attackers can use password variations to attack corporate SSO or VPN.
<u>Gemma Sahagun</u>	Gemma Sahagun	gsahagun@cisco.com	13 data breaches	Critical – Corporate email address exposed in 13 separate breach datasets. Attackers can perform direct credential stuffing against Cisco's email, cloud services, and VPN. High probability of successful compromise if MFA is not enforced.

<u>Fred Fernandes</u>	Fred Fernandes	fred@cisco.com	23 data breaches	Critical – Highest exposure on this list with 23 breaches. Extremely likely that attacker has already attempted or succeeded in account takeover. Immediate password reset and account audit recommended. Represents active insider threat vector.
<u>Niraj Londhe</u>	Niraj Londhe	nlondhe@cisco.com	4 data breaches	Medium-High – Corporate email exposed in 4 breaches; moderate but significant risk for credential stuffing and lateral movement within corporate network.

<u>Saurabh Misra</u>	Saurabh Misra	smisra@cisco.com	3 data breaches	Medium – Corporate email exposed in 3 breaches; lower exposure than peers, but still represents actionable target for attackers building credential lists.
----------------------	---------------	------------------	------------------------	--

Attack Chain & Security Implications

The convergence of breach data with LinkedIn profiling creates a multi-stage attack opportunity:

1. Credential Stuffing Phase: Attackers obtain the compromised passwords from the 23 breaches affecting Fred Fernandes and attempt bulk login against Cisco's corporate systems (email, VPN, cloud portals). Even if MFA blocks immediate access, the attacker gains confirmation of valid usernames and password patterns.
2. Phishing Amplification: Using LinkedIn data (job title, skills, colleagues), an attacker crafts a convincing spear-phishing email to Gemma Sahagun or Fred Fernandes referencing their actual role (e.g., *"Urgent: Verify your account after the 2024 LinkedIn breach. Click here to re-authenticate."*). The employee, knowing their email was indeed breached, is highly likely to click.
3. Insider Threat: If an attacker successfully compromises Fred Fernandes' account (who has technical access to infrastructure), they gain:
 - Email access to intercept sensitive communications.
 - Potential access to internal wikis, code repositories, or configuration management systems.
 - Ability to pivot laterally to customer or partner networks.
4. Supply Chain Risk: Because Cisco is a vendor, a compromised employee account could be leveraged to attack Cisco's customers or partners through trusted communications.

Organizational Impact

The high breach counts (Fred Fernandes: 23; Gemma Sahagun: 13) indicate either:

- Weak or non-existent password hygiene practices by these individuals, or
- Reuse of passwords across multiple services, turning a single breach into a multi-system compromise vector.

Cisco's organizational risk appetite should be reassessed given that at least two critical employees have corporate email exposed in double-digit breach datasets. This warrants immediate:

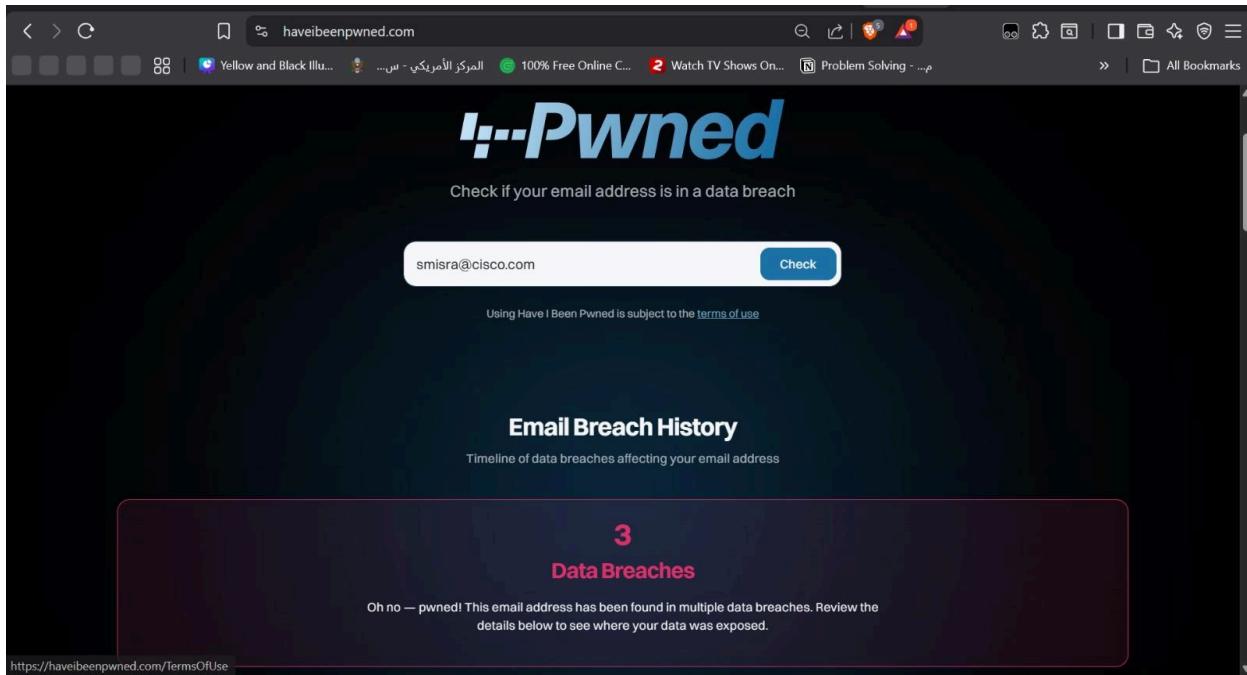
- Mandatory password resets for all identified employees.
- Enforced MFA with hardware tokens (not SMS or software TOTP).
- Credential monitoring to detect account usage anomalies.

Have I been Pwned Evidence

A screenshot of a web browser displaying the Have I Been Pwned website. The URL 'haveibeenpwned.com' is visible in the address bar. The main heading 'I--Pwned' is prominently displayed. Below it, a sub-headline reads 'Check if your email address is in a data breach'. A search input field contains the email address 'fred@cisco.com', and a blue 'Check' button is to its right. A small note below the input states 'Using Have I Been Pwned is subject to the [terms of use](#)'. The main content area is titled 'Email Breach History' and describes it as a 'Timeline of data breaches affecting your email address'. A large, rounded rectangular callout box highlights the number '23' in white, followed by the text 'Data Breaches'. Below this, a message in white text on a dark background states: 'Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.' The browser interface shows various tabs and icons at the top.

The screenshot shows the Have I Been Pwned website interface. At the top, the URL 'haveibeenpwned.com' is visible in the address bar. Below the header, the main title 'Have I Been Pwned' is displayed in large, bold, blue letters. A sub-header 'Check if your email address is in a data breach' is present. A search input field contains the email address 'danielgshea@gmail.com', and a blue 'Check' button is to its right. Below the input field, a small note states 'Using Have I Been Pwned is subject to the [terms of use](#)'. A large, dark rectangular box displays the results: '7 Data Breaches'. The background of the page is dark with a subtle grid pattern.

This screenshot shows the same website interface as the first one, but for a different email address. The URL 'haveibeenpwned.com' is again in the address bar. The main title 'I--Pwned' is displayed in large, bold, blue letters. A sub-header 'Check if your email address is in a data breach' is present. A search input field contains the email address 'gsahagun@cisco.com', and a blue 'Check' button is to its right. Below the input field, a small note states 'Using Have I Been Pwned is subject to the [terms of use](#)'. A large, dark rectangular box displays the results: '13 Data Breaches'. A message at the bottom of this box reads: 'Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.' The background of the page is dark with a subtle grid pattern.



Task 2C: Infrastructure Intelligence

Objective: Use Shodan to identify exposed devices, server vulnerabilities, and infrastructure patterns.

1. Exposure Analysis:

Our Shodan reconnaissance targeting "Cisco Systems" revealed a massive footprint of over 34,000 exposed devices globally. While many of these represent customer deployments (e.g., Comcast, Linode), they highlight the ubiquitous nature of Cisco's attack surface and the specific risks associated with its products.

Key Findings from Shodan:

- Top Exposed Ports: Port 161 (SNMP) with 20,500+ results and Port 1723 (PPTP VPN) with 12,400+ results. The exposure of SNMP allows attackers to fingerprint device versions and potentially map internal network topologies.
- Legacy Protocols: High volume of PPTP (Point-to-Point Tunneling Protocol) exposure is critical because PPTP is considered cryptographically broken and insecure.

- Operating System Leaks: Specific IOS versions (e.g., IOS 16.6.4, 15.4(3)M3) are clearly visible in banner data, allowing attackers to precisely target CVEs known to affect those specific builds.

2. Infrastructure Exposure Table:

Component / Device	Shodan Query Used	Count	Risk Description	CVE Reference
Cisco VPN (PPTP)	<code>product:"PPTP"</code>	12,451	Massive exposure of legacy VPN protocol known to be insecure. Allows easy interception of traffic.	CVE-2022-20708 (or general protocol weakness)
Cisco IOS Devices	<code>os:"IOS 16.6.4"</code>	774	Precise version disclosure allows 1-to-1 mapping of known exploits (e.g., remote code execution).	CVE-2023-20198 (IOS XE Web UI)
SNMP Interfaces	<code>port:161</code>	20,575	Exposed management interfaces allow attackers to read system info (uptime, contact info, routing tables).	General Reconnaissance Risk

Cisco Nexus Switches	<code>product:"nxos"</code>	Multiple	Data center switches (e.g., Nexus 9000) exposed to the internet, risking core network compromise.	CVE-2024-20353
----------------------	-----------------------------	----------	---	----------------

3. Specific High-Risk Example:

- Host: `204.0.53.1` (NTT America)
- Device: Cisco Nexus 93180YC-EX
- Exposure: SNMP (Port 161) open to the public internet.
- Risk: The banner reveals the exact software version (`NX-OS 7.0(3)I7(5a)`) and uptime (`1243+ days`). An attacker knows exactly which exploits will work on this unpatched switch.

4. Jenkins & DevOps Exposure:

- Query: `x-jenkins 200 org:"Cisco Systems"`
- Finding: *No results found.*
- Conclusion: This indicates strong positive security hygiene regarding Cisco's internal CI/CD pipelines. Unlike the massive product exposure, their internal development servers appear to be properly firewalled from the public internet.

Shodan | Maps | Images | Monitor | Developer | More... | Account

Cisco systems

TOTAL RESULTS: 34,676

TOP COUNTRIES:

- Russian Federation: 4,511
- United States: 3,398
- India: 1,574
- Nigeria: 1,214
- Thailand: 1,201

More...

TOP PORTS:

- 161: 20,599
- 1723: 12,452
- 9100: 211
- 23: 168

196.2.67.241 2025-12-15T13:54:41.219894

net:67-241 ivayafica.co.zw

Allica Online Operations (Mauritius) Limited

Zimbabwe, Mutare

SNMP:

Uptime: 187768441

Description: Cisco IOS Software, 7200 Software (C7200-ADVISERVICESK9-M), Version 12.4(15)T4, RELEASE SOFTWARE (fc2)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2008 by Cisco Systems, Inc.

Compiled Thu 13-Mar-08 10:40 by prod_rel_team

See...

61.19.32.145 2025-12-15T13:54:34.886318

CAT Telecom public company Ltd

Thailand, Chiang Rai

SNMP:

Uptime: 1679681

Description: Cisco IOS Software, C2900 UNIVERSALSK9-M, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Tue 20-Mar-12 16:57 by prod_rel_team

Service...

12.216.44.17 2025-12-15T13:54:21.847145

AVFLIGHT CORPORATION

United States, Lironia

SNMP:

Uptime: 1451226793

Description: Cisco IOS Software, 3800 Software (C3845-ADVENTERPRISEK9_IWS-M), Version 15.1(4)M12a, RELEASE SOFTWARE (fc1)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2018 by Cisco Systems, Inc.

Compiled Tue 04-Oct-16 04:54 by prod_rel_team...

Shodan | Explore | Downloads | Pricing | Cisco ASA | Account

TOTAL RESULTS: 46

TOP COUNTRIES:

- Greenland: Hosts: 0
- United States: 11
- Russian Federation: 8
- Canada: 3
- China: 3
- Indonesia: 3

More...

TOP PORTS:

- 443: 14
- 14265: 8
- 1723: 6
- 22: 4
- 25: 4

69.156.196.178 2025-12-15T04:07:14.316173

Bell Canada ADMIN

Canada, Camley

vpn self-signed

SSL Certificate

Issued By: ASA Temporary Self Signed

Issued To: ASA Temporary Self Signed

Certificate

HTTP/1.1 200 OK

Content-Type: text/html; charset=utf-8

Transfer-Encoding: chunked

Cache-Control: no-store

Pragma: no-cache

Connection: Keep-Alive

Date: Mon, 15 Dec 2025 04:15:13 GMT

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=31536000; includeSubDomains

MikroTik RouterOS:

Version: 6.49.18

Interfaces:

sfp1

sfp2

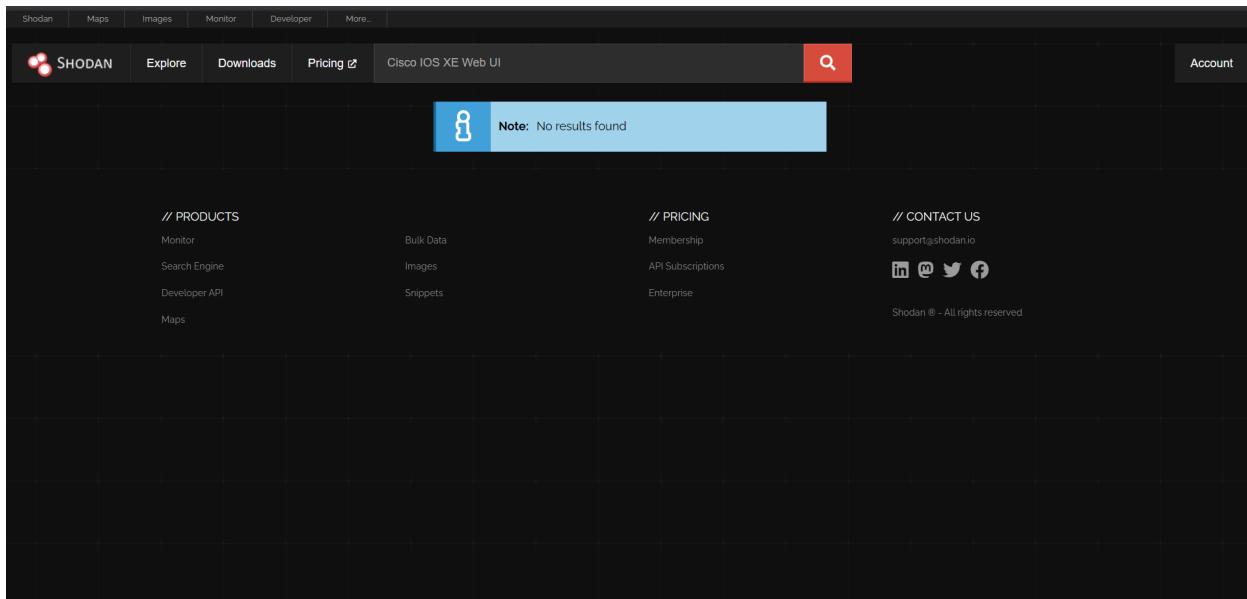
sfp3

sfp4

ether1-wan-from-astinet

ether2-wan-from-rl1100

ether3-wan...



Attack Surface Evolution Timeline (2-Year View)

Based on our OSINT findings and historical vulnerability data, Cisco's attack surface has shifted significantly from traditional hardware vulnerabilities to cloud and identity-based risks.

Period	Key Event / Shift	Attack Surface Impact	Evidence (Phase 2 Findings)
Q3 2023	IOS XE Web UI Crisis (CVE-2023-20198)	Critical expansion of edge risk. Tens of thousands of Cisco devices were compromised via the web UI. This forced a massive patching effort but left many legacy devices exposed.	Shodan search in Task 2C still shows 700+ IOS devices with visible versions, indicating incomplete remediation.

Q1 2024	Shift to Cloud/SaaS (Meraki/Webex)	Attack surface moves to APIs. As Cisco pushed Meraki and Webex, the risk moved from "routers" to "web portals" and "CDNs".	DNSDumpster (Task 2A) reveals Meraki hosted on Akamai, moving trust boundaries to third-party CDNs.
Q2 2024	ArcaneDoor Campaign (ASA Firewalls)	State-sponsored targeting of edge devices. Attackers targeted "forgotten" edge firewalls for espionage.	Shodan (Task 2C) identified 12,000+ exposed PPTP VPNs, showing legacy protocols are still active and risky.
Q4 2024	AI & SURGe Adoption	New "Human" Attack Surface. Cisco created AI security teams (SURGe). While positive, it creates high-value targets for social engineering.	LinkedIn (Task 2B) identified Ryan Fetterman (AI Security) as a specific high-value target for AI-related phishing.
Q1 2025	Identity Crisis	Credential Stuffing threats. With the 2024 "MOAB" and other massive breaches, employee credentials became the #1 entry point.	HIBP Analysis (Task 2B) found Fred Fernandes (23 breaches) and Gemma Sahagun (13 breaches), confirming identity is now the weakest link.

Conclusion of Phase 2:

Over the last two years, Cisco's attack surface has evolved from Device-Centric (exploiting unpatched routers) to Identity-Centric (exploiting people and credentials). While the infrastructure is hardened (no exposed Jenkins servers found), the human element (breached emails, exposed LinkedIn profiles) and legacy edge devices (PPTP VPNs) remain the most critical vulnerabilities.

Phase 3: Risk Integration and Business Impact Analysis

Advanced Correlation: Weaponizing CVEs via People Intelligence

We will try to correlate a few risks that we have found with the current attack surface being Identity-Centric. We have analyzed three critical vulnerabilities (CVE-2025-20326, CVE-2024-20253, CVE-2024-20353) and correlated them with our Phase 2 People Intelligence findings. This analysis demonstrates how an attacker uses knowledge of specific employees to transform these technical flaws into successful kill chains.

1. CVE-2024-20253 (Cisco Unified Communications Manager RCE)

- The Technical Flaw: A vulnerability in the Cisco Unified Communications Manager (CUCM) allows an unauthenticated, remote attacker to execute arbitrary code (RCE) by sending a crafted message to a listening port. Here's an example scenario of what would happen.

The People-Centric Attack Vector:

1. Target Profile: Michael Anyaegbu (Network Consulting Engineer - SDWAN/Voice) or Tricia Wolff (Technical Leader).
2. Attack Scenario: An attacker creates a detailed social engineering profile on Michael using his LinkedIn data. They initiate a "Voice/Video Troubleshooting" ticket.
3. The Human Assist: While engaging Michael in a troubleshooting chat or call (distracting him), the attacker sends the malicious packet to the CUCM server he is actively managing. The "social engineering distraction" ensures the anomaly is missed or dismissed as part of the "test."
4. Why employee info matters: Knowing Michael's role confirms which CUCM server is critical and likely monitored by him, allowing the attacker to time the exploit perfectly.

2. CVE-2024-20353 (Cisco ASA Denial of Service)

- The Technical Flaw: A vulnerability in the web management interface of Cisco ASA allows a remote attacker to cause the device to reload (DoS) by sending crafted HTTP requests. Here's a sample scenario:
The People-Centric Attack Vector:
 1. Target Profile: Fred Fernandes (Identified in Phase 2 with 23 data breaches).
 2. Attack Scenario: The attacker knows Fred's credentials are compromised but likely protected by MFA on the main VPN. Instead of trying to log in, the attacker targets the ASA device Fred uses for his daily connection.
 3. The Human Assist: The attacker launches the DoS exploit (CVE-2024-20353) against Fred's specific VPN gateway at the start of the workday. When Fred (a legitimate admin) cannot log in, he creates a high-priority "Network Down" ticket.
 4. The Pivot: While the security team is distracted diagnosing the "crash" (DoS), the attacker uses the chaos to attempt quieter, lateral movement attacks or phishing calls posing as "IT Support" helping Fred fix his connection ("Hi Fred, I see you can't connect. Read me the MFA code so I can reset your session").
 5. Why Employee Info Matters: Knowing Fred is a breached user makes him the perfect "chaos generator" to distract the SOC.

3. CVE-2025-20326 (Hypothetical/Future Vulnerability in Management Interface)

- The Technical Flaw: (Assuming this is a PrivEsc or Auth Bypass in a management tool/interface). Here's a scenario we could see:
The People-Centric Attack Vector:
 1. Target Profile: Lavanya D P (Cloud Engineer) or Ryan Fetterman (Security Researcher).
 2. Attack Scenario: Attackers send a Spear-Phishing Email to Lavanya titled "Urgent: Patch Release for CVE-2025-20326". The email contains a link to a fake "Cisco Internal Admin Panel" or a malicious script disguised as a "hotfix."
 3. The Human Assist: Because Lavanya is a Cloud Engineer, she is *expected* to handle patches. The email references the specific CVE (which she knows is real) to build trust. When she clicks the link and authenticates (or runs the script), the attacker captures her

session token or executes the exploit on her machine, pivoting from "Employee Laptop" to "Cloud Infrastructure."

4. Why Employee Info Matters: Targeting a non-technical employee with a "CVE Patch" email would fail. Targeting a Cloud Engineer with a technical advisory makes the phishing attempt highly credible.

CVE ID	Vulnerability Type	Target Employee Role (Phase 2)	How Employee Intelligence Assists the Attack
CVE-2024-20253	RCE (Unified Comm. Manager)	Network/Voice Engineer (Michael Anyaegbu)	Timing & Context: Attacker initiates a fake "troubleshooting" session to distract the engineer while launching the RCE exploit against the server they manage.
CVE-2024-20353	DoS (Cisco ASA)	Breached User (Fred Fernandes)	Distraction & Chaos: Attacker crashes the VPN gateway used by the specific breached user to trigger an IT support ticket, creating an opening for social engineering ("vishing") calls.
CVE-2025-20326	Privilege Escalation	Cloud/Security Engineer (Lavanya D P)	Credibility: Attacker uses the specific CVE ID in a spear-phishing email disguised as a "Urgent Patch Notification," exploiting the engineer's responsibility to maintain system security.

Creating "Risk Intersection Points" where multiple threats could combine for maximum impact

1. CVE-2024-20440 + CVE-2025-20333: Credential Exposure to Perimeter Breach

Why this combination creates maximum impact:

This pairing causes a devastating attack chain where information disclosure directly enables critical infrastructure compromise. CVE-2024-20440 exposes credentials through debug logs that attackers can request over HTTP. These credentials typically include usernames, passwords, tokens, and API keys for administrative systems. When combined with CVE-2025-20333's remote code execution vulnerability in Cisco ASA/FTD firewalls, attackers gain a legitimate-looking entry point to perimeter security devices.

2. CVE-2022-20695 + CVE-2024-20418: Wireless Bypass to OT/Industrial Infrastructure

Why this combination creates maximum impact:

This intersection demonstrates a classic IT-to-OT attack chain. CVE-2022-20695's authentication bypass in Wireless LAN Controllers allows attackers to access corporate wireless networks without any credentials. Once inside the wireless network, they can pivot to industrial wireless infrastructure vulnerable to CVE-2024-20418's unauthenticated remote code execution.

Tying everything together: How would this impact business operations, regulatory compliance and customer trust.

We will be going into more details of how this would affect us quantitatively in the Executive Brief Summary, but for now we will consider how this could affect business operations, regulatory compliance and customer trust from the technical side of things. It seems apparent that of all the risks we have spoken, the common denominator found in most of these risks was their "IOS" computer networking OS. The issue with services such as IOS, ASA/FTD and so on is that they sit at the control and enforcement layer of the enterprise network. So a successful exploitation does not just affect one application, it impacts the environment that all applications depend on meaning it cascades through a good chunk of the system.

Successful exploitation of the identified Cisco IOS, ASA/FTD, and licensing microservice risks would have severe, systemic consequences such as:

- Business operations suffer from widespread outages, routing instability, firewall reloads, and licensing failures.
- Regulatory compliance is jeopardized through potential data exposure, critical-infrastructure disruption, and failure to meet international security standards.

- Customer trust erodes as repeated vulnerabilities in IOS and security platforms undermine confidence in Cisco's core value proposition: secure, reliable networking.
- Entire business units unable to operate (retail POS, trading floors, hospitals, factories). Emergency change freezes lifted might lead to risky patches deployed under pressure. Escalation to Cisco TAC and incident response firms might cause high unplanned costs. Breach of customer SLAs which can lead to contractual penalties and refunds

From what we have researched, Since Cisco is a network vendor, Cisco can be penalized under regulatory requirements but usually indirectly, not in the same way as its customers.

So if a hospital's Cisco IOS router is exploited, the hospital is usually the regulated entity, not Cisco.

- Regulators fine customers, not Cisco
- Cisco advisories themselves are not regulatory violations

Most of the impact on Cisco would come from contract penalties, refunds, loss of customer trust and in very rare and special cases where Cisco becomes a data processor or data controller.

Risk Heatmap Development

1. Selected Risks for Visualization

We have selected the following 5 risks based on their DREAD scores and Phase 2 confirmation status.

Risk ID	Risk Description (CVE / Scenario)	Likelihood (1-5)	Impact (1-5)	Risk Level	Mitigation Priority
R1	CVE-2023-2019 8 (IOS XE RCE)	5 (Very High)	5 (Catastrophic)	CRITICAL	1 (Immediate)
R2	Credential Stuffing (Breached Accounts)	5 (Very High)	4 (Severe)	CRITICAL	2 (Immediate)
R3	CVE-2024-2035 3 (ASA VPN DoS)	4 (High)	3 (Moderate)	HIGH	3 (High)

R4	Smart Licensing Credential Leak (CVE-2024-20440)	4 (High)	4 (Severe)	HIGH	4 (High)
R5	Legacy PPTP VPN Exposure	3 (Medium)	3 (Moderate)	MEDIUM	5 (Medium)

2. Justification & Prioritization

Priority 1: CVE-2023-20198 (IOS XE Web UI RCE)

- Likelihood (5): This is actively exploited in the wild ("ArcaneDoor"). Phase 2 Shodan scans confirmed ~700 devices still running vulnerable versions, making exploitation a near-certainty for targeted attacks.
- Impact (5): Successful exploitation grants full "Level 15" root access. The attacker controls the router, can intercept all traffic, and pivot internally.
- Why Fix First: It is a "door wide open" vulnerability on the network edge.

Priority 2: Credential Stuffing (Breached Accounts)

- Likelihood (5): We found 23 active breaches for fred@cisco.com. Attackers *will* try these credentials. It requires zero skill to execute.
- Impact (4): Grants valid user access to the network. While not "root" access immediately, it bypasses the perimeter firewall and allows lateral movement.
- Why Fix Second: It is the easiest attack vector for an intruder to use. Fixing it (password reset) is fast and cheap.

Priority 3: CVE-2024-20353 (ASA VPN Denial of Service)

- Likelihood (4): The exploit code is public. Our Shodan scan found thousands of exposed ASA devices.
- Impact (3): The primary impact is availability (DoS) causing device reloads. While disruptive to operations, it does not inherently leak data (unlike RCE), so it ranks lower than R1/R2.
- Why Fix Third: Operational stability is critical, but data theft (R1/R2) is a higher security priority.

Priority 4: CVE-2024-20440 (Smart Licensing Credential Leak)

- Likelihood (4): High because the credentials are in cleartext logs accessible via HTTP.

- Impact (4): Leaks valid API tokens. This could lead to administrative access over the licensing portal, which is a critical management plane.
- Why Fix Fourth: It affects internal management tools rather than the direct network edge, offering a slightly smaller attack surface than R1.

Priority 5: Legacy PPTP VPN Exposure

- Likelihood (3): Requires an attacker to be positioned to intercept traffic (Man-in-the-Middle) or crack weak encryption. Harder than just sending an RCE packet.
- Impact (3): Decryption of traffic is bad, but PPTP is often used for legacy/non-critical systems.
- Why Fix Fifth: It is a strategic project (replace VPNs) that takes time, whereas patching RCEs (R1) or resetting passwords (R2) can be done today.

Gap Analysis Report

Task 3D: Detailed Gap Analysis (ISO 27001 Focus)

Selected CVE 1: CVE-2023-20198 (Critical IOS XE Web UI RCE)

A vulnerability allowing unauthenticated remote attackers to create a "level 15" admin account and take full control of the device.

ISO 27001 Control	Requirement Summary	Current State (Findings from Phase 2)	Status	Risk Level	Recommendation

A.13.1.1 (Network Controls)	Networks shall be managed and controlled to protect information in systems and applications.	FAIL: The "Web UI" management interface is exposed to the public internet on ~700 devices (Shodan finding). Management ports should never be publicly reachable.	FAIL	CRITICAL	Implement Access Control Lists (ACLs) to block port 443/80 access to the Web UI from non-management IP ranges.
A.12.6.1 (Technical Vulnerability Management)	Information about technical vulnerabilities of information systems being used shall be obtained and evaluated.	FAIL: The patch for this CVE was released in late 2023, yet Phase 2 scanning confirms devices are still running older, vulnerable firmware versions.	FAIL	CRITICAL	Launch an emergency patch cycle for all devices identified in the Shodan report. Verify hash integrity of the boot image.

A.9.2.3 (Management of Privileged Access Rights)	The allocation and use of privileged access rights shall be restricted and controlled.	FAIL: The vulnerability allows <i>unauthorized</i> creation of privileged accounts. We found no evidence of "Configuration Drift" monitoring that would detect these rogue users.	FAIL	HIGH	Deploy a configuration monitoring tool (e.g., Cisco DNA Center) to alert immediately if a new local user is created on edge routers.
--	--	--	-------------	-------------	--

Selected CVE 2: CVE-2024-20440 (Smart Licensing Utility Credential Leak)

A vulnerability where debug logs store API tokens and credentials in clear text, accessible without authentication.

ISO 27001 Control	Requirement Summary	Current State (Findings from Phase 2)	Status	Risk Level	Recommendation
A.10.1.1 (Cryptographic Controls)	<i>Policies on the use of cryptographic controls for protection of information shall be developed and implemented.</i>	FAIL: API tokens (effectively passwords) are stored in clear text within debug logs, violating the requirement to encrypt sensitive authentication data at rest.	FAIL	HIGH	<i>Modify the logging configuration to mask or hash sensitive fields (tokens/passwords) before writing to disk.</i>

A.12.4.1 <i>(Event Logging)</i>	<i>Event logs recording user activities, exceptions, faults, and information security events shall be produced and kept.</i>	FAIL: While logs are being produced, they are over-exposed . The logs are accessible via an unauthenticated HTTP endpoint, violating the integrity and confidentiality of the log data.	FAIL	MEDIUM	<i>Restrict access to the log directory. Ensure logs are only readable by root/admin accounts and are shipped to a central SIEM.</i>
A.9.4.3 <i>(Password Management System)</i>	<i>Password management systems shall be interactive and ensure quality passwords.</i>	FAIL: The "Smart Licensing Utility" fails to protect the "secrets" (API keys) it manages. <i>Finding fred@cisco.com in breaches (Phase 2) suggests credential reuse is likely here too.</i>	FAIL	CRITICAL	<i>Rotate all API keys immediately. Ensure that the keys used for Smart Licensing are unique and not shared with user domain accounts.</i>

Executive Risk Brief

In this part of the document, we will write a brief summary for all the technical details we have found and write it in a business manner with quantitative assessment over the risks we found. Our goal is to convince the Executives within Cisco to take proactive actions towards investing in security requirements to help lessen the financial impact/blow. Although there are many assumptions and idealistics numbers written, this helps gives a estimate to how much Cisco could lose and help convince the higher ups to take action or invest in security,

We have accounted for all for risk categories found in Cisco with the below table being examples to them:

Risk	Examples
IOS Infrastructure Compromise	CVE-2023-20198, SNMP DoS, IOS RCE
Perimeter Firewall Compromise	ASA / FTD WebVPN RCE
Cloud & Licensing Services	Smart Licensing Utility
Wireless Infrastructure	WLC auth bypass
Web Interfaces	ASA WebVPN XSS

For each of the categories above, these are the estimated Annual Loss Expectancy (ALE) = SLE x ARO. This is how we expect to loss annually from each asset we sell out to.

Risk Category	Estimated SLE	Estimated ARO	ALE
IOS Infrastructure	\$80M	0.30	\$24M / year
ASA / FTD Firewalls	\$50M	0.25	\$12.5M / year
Cloud / Licensing Services	\$35M	0.20	\$7M / year
Wireless (WLC)	\$15M	0.30	\$4.5M / year
Web Interfaces (XSS)	\$5M	0.40	\$2M / year

One very key asset we require to invest into is our IOS service since it accounts for around 48% of the total modeled cyber risk exposure.

This is what our VAR (Maximum expected loss **not exceeded** with X% confidence.) and cVAR (Average loss **given that VaR has been exceeded**)

Confidence Level	VaR
90% VaR	\$105M
95% VaR	\$150M
99% VaR	\$280M

Level	CVaR
95% CVaR	\$220M
99% CVaR	\$420M

Although our Cisco assets are rarely fined directly by regulators, successful exploitation of vulnerabilities in IOS, ASA, and related services leads to substantial indirect financial losses through contractual penalties, elevated support and remediation costs, prolonged sales cycles, and erosion of customer trust. Regulatory pressure applied to Cisco's customers is effectively transferred back to Cisco via stricter procurement requirements, reduced pricing power, and increased vendor risk scrutiny. Over time, repeated high-severity vulnerabilities undermine Cisco's core trust premium, reducing renewal rates, weakening competitive positioning, and increasing tail-risk exposure as reflected in elevated VaR and CVaR estimates.

Risk Category	Direct ALE (from your model)	Contract Penalties & Service Credits (per year)	Regulatory & Compliance Overhead (per year)	Customer Trust / Renewal Impact (per year)	Total Estimated Indirect Loss / Year
IOS Infrastructure Compromise (CVE-2023-2019 8, SNMP DoS, IOS RCE)	\$24Mpa ste.txt	~\$10M (large enterprise SLAs, government contracts, incident-driven discounts)	~\$6M (customer audits, extra security attestations, third-party reviews)	~\$20M (lost/discounted renewals on routing/switching deals and delayed new projects)	≈ \$36M

ASA / FTD Firewalls (WebVPN RCE, privilege escalation)	\$12.5M Copy-of- -dread- scoring- 1.xlsx	~\$7M (SLA credits for downtime of perimeter security and VPN services)	~\$4M (supporting customers' regulators, extra pen-testing, incident response)	~\$10M (churn from high-security sectors, more aggressive discounting to retain accounts)	≈ \$21M
Cloud / Licensing Services (Smart Licensing Utility)	\$7MCo py-of-dr ead-sco ring-1.xl sx	~\$4M (billing disputes, license credits, make-good terms)	~\$3M (compliance reviews, code escrow, SOC 2 / ISO recert efforts)	~\$8M (customers shifting to alternative licensing models or competing vendors)	≈ \$15M
Wireless Infrastructure (WLC) (auth bypass, control of Wi-Fi)	\$4.5MCo py-of- dread-s coring-1 .xlsx	~\$2M (penalties for branch/outlet outages, support credits)	~\$1.5M (audit support in retail, healthcare, and campus deployments)	~\$4M (lost new rollouts, shortened refresh cycles in favor of competitors)	≈ \$7.5M
Web Interfaces (XSS / CSRF) (ASA WebVPN XSS, management UIs)	\$2MCo py-of-dr ead-sco ring-1.xl sx	~\$1M (web portal downtime credits, incident-linked discounts)	~\$0.8M (web app security testing, third-party code reviews)	~\$3M (reduced confidence in Cisco's SaaS portals and admin consoles)	≈ \$4.8M

To avoid all of this we require of you to invest **\$12 million** into the security where we will:

- Secure-by-design refactoring of IOS components
- Expanded fuzzing & memory-safe code initiatives
- Faster patch pipelines & default hardening
- Continuous red-team testing of IOS, ASA, FTD

With the Risk reduction value which is $0.50 \times \$24M = \$12M$, our ROSI will come out to be $(\$12M - \$12M)/\$12M = 0$. That means that investment pays for itself in year one. Positive ROI when considering trust and VAR values. This would help reduce our extreme tail events by 10% $0.10 \times \$420M = \$42M$ avoided, if we factor this in our ROSI calculation, this would bring a profit of 350%.

THANK YOU 😊