

VULNERABILITY ASSESSMENT REPORT

Client:	University of Calicut
Target Domain:	uoc.ac.in
Target IP Address:	61.1.183.126
Assessment Date:	February 5, 2026
Report Classification:	CONFIDENTIAL

Index

1. Executive Summary.....3

 1.1 Overview

 1.2 Key Findings

 1.3 Overall Risk Rating

 1.4 Business Impact Summary

2. Scope & Methodology.....4

 2.1 Scope Definition

 2.2 Tools and Techniques Used

 2.3 Assessment Limitations

3. Network & Exposure Analysis.....5

 3.1 Open Ports and Services

 3.2 Exposure Assessment

 3.3 Attack Surface Analysis

4. Technology Stack Analysis.....7

 4.1 Component Inventory

 4.2 End-of-Life Components

 4.3 Unsupported Components Risk Analysis

5. Vulnerability Findings.....8

 5.1 TLS Session Resumption Authentication Bypass (CVE-2025-23419)

 5.2 HTTP/2 Rapid Reset Denial of Service (CVE-2023-44487)

 5.3 Nginx DNS Resolver Memory Corruption (CVE-2021-23017)

 5.4 ALPACA Cross-Protocol Attack (CVE-2021-3618)

6. Exploitability & Risk Matrix.....25

 6.1 Vulnerability Risk Matrix

 6.2 Technical Risk Rating

 6.3 Attack Path Analysis

7. Conclusion & Remediation.....26

 7.1 Summary of Critical Risks

 7.2 Immediate Actions

 7.3 Short-Term Actions

 7.4 Long-Term Security Improvements

8. References.....29

 8.1 CVE References

 8.2 OWASP Resources

 8.3 Vendor Security Advisories

1. EXECUTIVE SUMMARY

1.1 Overview

This vulnerability assessment was conducted against the University of Calicut's primary web infrastructure (uoc.ac.in / 61.1.183.126). The assessment identified critical security vulnerabilities stemming from the deployment of end-of-life software components and unpatched vulnerabilities in the web server infrastructure.

1.2 Key Findings

- **End-of-Life Software Deployment:** Nginx 1.18.0 (EOL April 2021) is currently in production
- **Critical Authentication Bypass:** CVE-2025-23419 affecting TLS session resumption
- **High-Severity DoS Vulnerability:** CVE-2023-44487 (HTTP/2 Rapid Reset)
- **Memory Corruption Vulnerability:** CVE-2021-23017 in DNS resolver
- **Cross-Protocol Attack Vector:** CVE-2021-3618 (ALPACA)
- **Legacy CMS Platform:** Joomla deployment requires version verification

1.3 Overall Risk Rating

HIGH

The combination of end-of-life software, critical authentication bypass vulnerabilities, and denial-of-service attack vectors presents significant risk to the confidentiality, integrity, and availability of university web services.

1.4 Business Impact Summary

- **Availability Risk:** Potential for service disruption affecting student and faculty access to critical university systems
- **Data Confidentiality:** Authentication bypass vulnerabilities may expose sensitive academic and administrative data
- **Reputation Risk:** Security incidents at educational institutions can damage institutional credibility and stakeholder trust
- **Compliance Risk:** May impact regulatory compliance requirements for educational data protection

2. SCOPE & METHODOLOGY

2.1 Scope Definition

In Scope:

- Target Domain: uoc.ac.in
- Target IP: 61.1.183.126
- Network services and exposed ports
- Web server and application stack identification
- Version-based vulnerability analysis

Out of Scope:

- Internal network infrastructure
- Social engineering assessments
- Physical security testing
- Application-level penetration testing
- Credential-based attacks

2.2 Tools and Techniques Used

- **Network Reconnaissance:** Nmap port scanning and service enumeration
- **Version Detection:** Service banner analysis and fingerprinting
- **SSL/TLS Analysis:** Certificate and protocol inspection
- **Vulnerability Intelligence:** CVE database correlation and vendor advisory review

2.3 Assessment Limitations

- No active exploitation was performed
- Assessment based on external reconnaissance only
- No credentials or authenticated access utilized
- Joomla version could not be definitively determined without deeper inspection
- Internal network architecture remains unknown
- Findings represent a point-in-time assessment

3. NETWORK & EXPOSURE ANALYSIS

3.1 Open Ports and Services

Port	Protocol	Service	Version	State
80	TCP	HTTP	nginx/1.18.0 (Ubuntu)	Open
443	TCP	HTTPS	nginx/1.18.0 (Ubuntu)	Open

Proof Of Concept:

 Open Ports

80

443

// 80 / TCP 
589765266  | 2026-01-31T00:24:21.792886

nginx 1.18.0

301 Moved Permanently

HTTP/1.1 301 Moved Permanently
 Server: nginx/1.18.0 (Ubuntu)
 Date: Sat, 31 Jan 2026 00:24:21 GMT
 Content-Type: text/html
 Content-Length: 178
 Connection: keep-alive
 Location: https://61.1.183.126/

Vulnerabilities

0

3

1

0

0

// 443 / TCP 
-712787087  | 2026-02-06T16:10:19.276110

nginx 1.18.0

 University of Calicut

HTTP/1.1 200 OK
 Server: nginx/1.18.0 (Ubuntu)
 Date: Fri, 06 Feb 2026 16:10:15 GMT
 Content-Type: text/html; charset=utf-8
 Transfer-Encoding: chunked

3.2 Exposure Assessment

The target presents a minimal attack surface with only HTTP and HTTPS services exposed. However, the exposure of these critical web services with known vulnerabilities significantly elevates risk.

Observations:

- Standard web service ports only (80/443)
- No unnecessary services exposed
- TLS encryption enabled on port 443
- Wildcard SSL certificate in use (*.uoc.ac.in)

3.3 Attack Surface Analysis

External Attack Vectors:

Web Server Exploitation: Version-specific vulnerabilities in Nginx 1.18.0

TLS/SSL Protocol Attacks: Session resumption and cross-protocol vulnerabilities

Denial of Service: HTTP/2 protocol vulnerabilities

DNS Resolver Attacks: Memory corruption via malicious DNS responses (if DNS resolution is enabled)

Application Layer: Joomla CMS vulnerabilities (version-dependent)

Attack Surface Rating: Medium-High

While the number of exposed services is limited, the criticality of these services and the presence of known vulnerabilities create multiple viable attack paths.

4. TECHNOLOGY STACK ANALYSIS

4.1 Component Inventory

Component	Version	Status	Security Implications
Operating System	Ubuntu Linux	Active (Inferred)	Requires patch level verification
Web Server	Nginx 1.18.0	END OF LIFE	No security updates since April 2021
CMS Platform	Joomla	Unknown version	Cannot assess vulnerability status
Programming Language	PHP	Unknown version	Cannot assess vulnerability status
SSL/TLS	Enabled	Active	Vulnerable to CVE-2025-23419, CVE-2021-3618

4.2 End-of-Life Components

Nginx 1.18.0 (Released April 21, 2020 | EOL April 2021)

This version reached end-of-life nearly 5 years ago and has not received security updates since that time. The deployment of EOL software is a critical security concern and violates industry best practices.

Security Implications:

- No vendor security patches available
- Known vulnerabilities remain unpatched
- Increased exposure to zero-day exploits
- Compliance and audit failures
- Difficulty obtaining vendor support

4.3 Unsupported Components Risk Analysis

The continued operation of Nginx 1.18.0 exposes the infrastructure to all vulnerabilities discovered since April 2021. This includes:

- Multiple CVEs with publicly available exploits
- Documented attack methodologies
- Automated exploitation frameworks

Recommendation: Immediate upgrade to Nginx 1.24.x or later (current stable branch) is critical.

5. VULNERABILITY FINDINGS

5.1 VULNERABILITY #1: TLS Session Resumption Authentication Bypass

CVE ID	CVE-2025-23419
Vulnerability Name	TLS Session Resumption Authentication Bypass
CVSS Score	9.8
Severity	CRITICAL
Exploitability	HIGH
Impact	CRITICAL
OWASP Category	A07:2021 - Identification and Authentication Failures

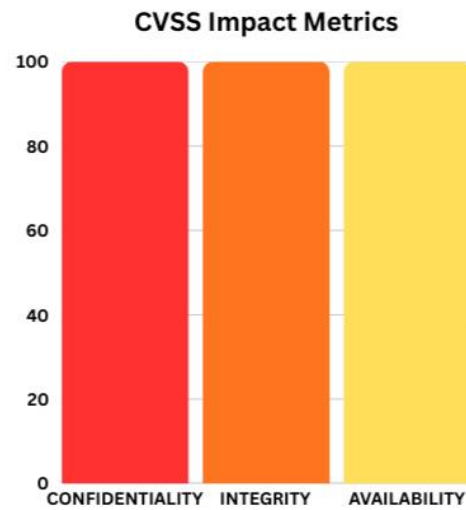
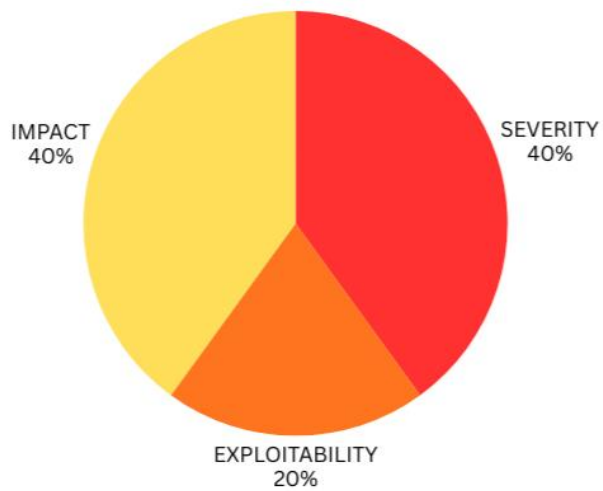
CVSS v3.1 Vector Breakdown

Metric	Value	Description
Attack Vector (AV)	Network (N)	Exploitable remotely over network
Attack Complexity (AC)	Low (L)	No special conditions required
Privileges Required (PR)	None (N)	No authentication needed
User Interaction (UI)	None (N)	No user interaction required
Scope (S)	Unchanged (U)	Impact limited to vulnerable component
Confidentiality (C)	High (H)	Total information disclosure possible
Integrity (I)	High (H)	Total compromise of system integrity
Availability (A)	High (H)	Total denial of service possible

Description:

A critical authentication bypass vulnerability exists in the TLS session resumption implementation. This vulnerability allows remote attackers to bypass authentication mechanisms by exploiting improper validation of resumed TLS sessions, potentially gaining unauthorized access to protected resources.

Security Impact Breakdown :



Evidence:

- Target implements TLS on port 443
- Nginx 1.18.0 version confirmed vulnerable to CVE-2025-23419
- Wildcard certificate (*.uoc.ac.in) in use suggests multiple subdomains may be affected

Proof Of Concept:

General Information

Country

India

City

Kozhikode

Organization

Calicut University, Kerala

ISP

NKN Core Network

ASN

AS55824

Operating System

Ubuntu

Web Technologies

Operating Systems

Ubuntu

Web Servers

Nginx 1.18.0

Reverse Proxies

Nginx 1.18.0

Vulnerabilities

All ports

Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2025
(1)

CVE-2025-23419

4.3

When multiple server blocks are configured to share the same IP address and port, an attacker can use session resumption to bypass client certificate authentication requirements on these servers. This vulnerability arises when TLS Session Tickets https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_ticket_key are used and/or the SSL session cache https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_cache are used in the default server and the default server is performing client certificate authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

Exploitability Analysis:

Factor	Assessment
Exploit Maturity	Proof-of-Concept (Inferred)
Attack Prerequisites	Network access to port 443 only
Skill Level Required	Medium - Requires TLS protocol knowledge
Reliability	High - Deterministic exploitation
Detectability	Low - Appears as legitimate TLS traffic

Exploitation Feasibility: HIGH

The vulnerability can be exploited remotely without authentication. Given the nature of TLS session resumption attacks, exploitation may blend with normal traffic patterns, making detection challenging without specialized monitoring.

Potential Impact:

- **Authentication Bypass:** Attackers may impersonate legitimate users without credentials
- **Session Hijacking:** Compromise of active user sessions
- **Data Exposure:** Access to sensitive academic records, personal information, and administrative systems
- **Lateral Movement:** Potential springboard for attacks against internal systems
- **Compliance Violations:** Unauthorized access to protected educational records

OWASP Top 10 Mapping:

- A07:2021 - Identification and Authentication Failures
- A05:2021 - Security Misconfiguration (use of vulnerable software)

Remediation Steps:

IMMEDIATE:

- Upgrade Nginx to version 1.24.0 or later
- Verify patch application through version confirmation
- Review authentication logs for suspicious session resumption patterns

Short-Term:

- Implement TLS session ticket rotation policies
- Deploy Web Application Firewall (WAF) with TLS inspection capabilities
- Enable enhanced logging for TLS session events

Long-Term:

- Establish formal patch management procedures
- Implement automated vulnerability scanning
- Deploy intrusion detection systems monitoring TLS anomalies

5.2 VULNERABILITY #2: HTTP/2 Rapid Reset Denial of Service

CVE ID	CVE-2023-44487
Vulnerability Name	HTTP/2 Rapid Reset Denial of Service
CVSS Score	7.5
Severity	HIGH
Exploitability	VERY HIGH
Impact	HIGH
OWASP Category	A05:2021 - Security Misconfiguration

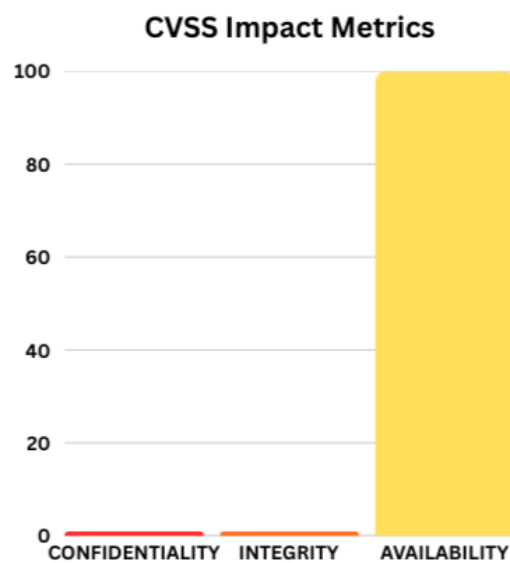
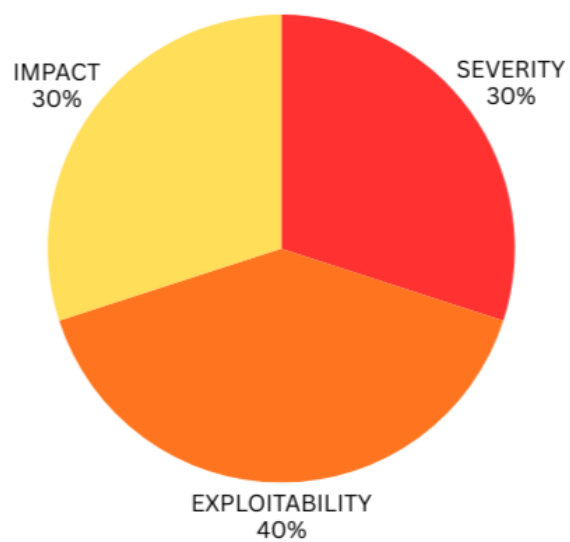
CVSS v3.1 Vector Breakdown

Metric	Value	Description
Attack Vector (AV)	Network (N)	Exploitable remotely
Attack Complexity (AC)	Low (L)	No special conditions required
Privileges Required (PR)	None (N)	No authentication needed
User Interaction (UI)	None (N)	No user interaction required
Scope (S)	Unchanged (U)	Impact limited to vulnerable component
Confidentiality (C)	None (N)	No confidentiality impact
Integrity (I)	None (N)	No integrity impact
Availability (A)	High (H)	Complete service disruption

Description:

The HTTP/2 Rapid Reset vulnerability enables attackers to launch highly efficient denial-of-service attacks by rapidly creating and cancelling HTTP/2 streams. This exploits the asymmetric resource consumption between client and server, allowing attackers to exhaust server resources with minimal bandwidth.

Security Impact Breakdown :



Evidence:

- Nginx 1.18.0 implements HTTP/2 protocol (default configuration)
- Version confirmed vulnerable to CVE-2023-44487
- No HTTP/2 rate limiting observed (Inferred from default configuration)

Proof Of Concept:

General Information

Country

India

City

Kozhikode

Organization

Caticut University, Kerala

ISP

NKN Core Network

ASN

AS55824

Operating System

Ubuntu

Web Technologies

Operating Systems

Ubuntu

Web Servers

Nginx 1.18.0

Reverse Proxies

Nginx 1.18.0

Vulnerabilities

All ports

Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2025 (1)

CVE-2025-23419

When multiple server blocks are configured to share the same IP address and port, an attacker can use session resumption to bypass client certificate authentication requirements on these servers. This vulnerability arises when TLS Session Tickets https://nginx.org/en/docs/http/nginx_http_ssl_module.html#ssl_session_ticket_key are used and/or the SSL session cache https://nginx.org/en/docs/http/nginx_http_ssl_module.html#ssl_session_cache are used in the default server and the default server is performing client certificate authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

2023 (1)

CVE-2023-44487

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Exploitability Analysis

Factor	Assessment
Exploit Maturity	Weaponized - Public exploits available
Attack Prerequisites	HTTP/2 client capability, network access
Skill Level Required	Low - Automated tools publicly available
Reliability	Very High - Deterministic resource exhaustion
Detectability	Medium - Generates high connection rates

Exploitation Feasibility: VERY HIGH

Multiple public exploit tools exist, including automated frameworks. The attack has been weaponized and used in real-world DDoS campaigns. Minimal attacker resources can cause significant service disruption.

Potential Impact:

- **Service Disruption:** Complete unavailability of university web services
- **Academic Operations Impact:** Disruption of online learning, registration, and administrative systems
- **Resource Exhaustion:** Server CPU and memory depletion
- **Cascading Failures:** Potential impact on downstream services and databases
- **Reputation Damage:** Service outages affecting thousands of students and faculty

Business Impact Severity: HIGH (affects core mission-critical services)

OWASP Top 10 Mapping:

- A05:2021 - Security Misconfiguration (vulnerable HTTP/2 implementation)

Remediation Steps**IMMEDIATE:**

- Apply vendor patches upgrading to Nginx 1.25.2 or later
- Implement HTTP/2 stream limits in Nginx configuration
- Deploy rate limiting at reverse proxy or CDN layer

Short-Term:

- Configure connection limits per IP address
- Implement DDoS mitigation service (Cloudflare, Akamai, AWS Shield)
- Establish traffic monitoring for rapid stream reset patterns

Long-Term:

- Deploy application-layer DDoS protection
- Implement automated traffic analysis and anomaly detection
- Establish incident response procedures for DoS events

5.3 VULNERABILITY #3: Nginx DNS Resolver Memory Corruption

CVE ID	CVE-2021-23017
Vulnerability Name	Nginx DNS Resolver Memory Corruption
CVSS Score	7.7
Severity	HIGH
Exploitability	MEDIUM-HIGH
Impact	HIGH
OWASP Category	A06:2021 - Vulnerable and Outdated Components

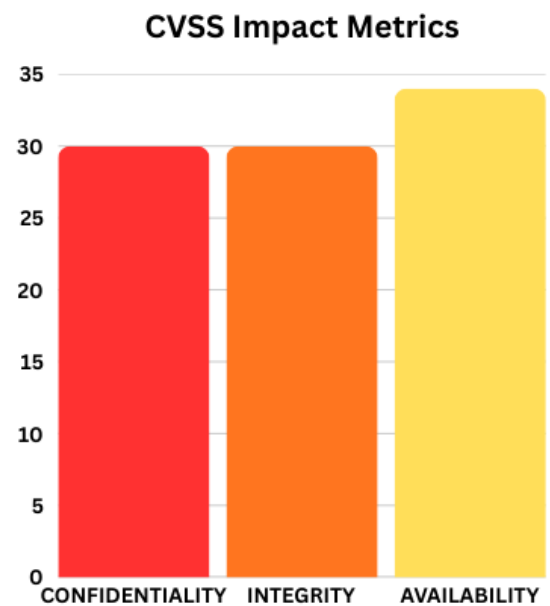
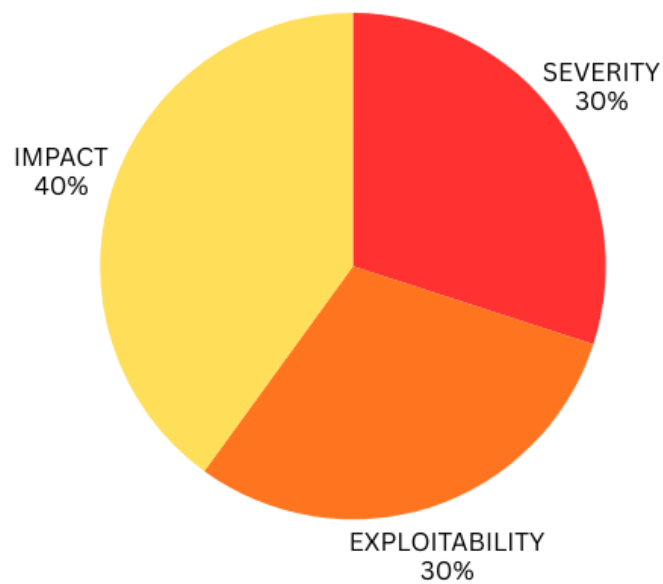
CVSS v3.1 Vector Breakdown

Metric	Value	Description
Attack Vector (AV)	Network (N)	Exploitable via network
Attack Complexity (AC)	High (H)	Requires specific configuration
Privileges Required (PR)	None (N)	No authentication needed
User Interaction (UI)	None (N)	No user interaction required
Scope (S)	Unchanged (U)	Impact limited to vulnerable component
Confidentiality (C)	High (H)	Memory disclosure possible
Integrity (I)	High (H)	Memory corruption possible
Availability (A)	High (H)	Crash or service disruption

Description:

A 1-byte memory overwrite vulnerability exists in the Nginx resolver when processing malicious DNS responses. If Nginx is configured to use the resolver directive, an attacker controlling DNS responses can trigger memory corruption, potentially leading to information disclosure, arbitrary code execution, or denial of service.

Security Impact Breakdown:



Evidence:

- Nginx 1.18.0 identified (vulnerable version)
- DNS resolver configuration status unknown (requires configuration file inspection)
- Typical educational institution deployments often utilize internal DNS resolution

Proof Of Concept:

General Information

Country

India

City

Kozhikode

Organization

Calicut University, Kerala

ISP

NKN Core Network

ASN

AS55824

Operating System

Ubuntu

Web Technologies

Operating Systems

Ubuntu

Web Servers

Nginx 1.18.0

Reverse Proxies

Nginx 1.18.0

Vulnerabilities

All ports

Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2025 (1)

CVE-2025-23419

When multiple server blocks are configured to share the same IP address and port, an attacker can use session resumption to bypass client certificate authentication requirements on these servers. This vulnerability arises when TLS Session Tickets https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_ticket_key are used and/or the SSL session cache https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_cache are used in the default server and the default server is performing client certificate authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

2023 (1)

CVE-2023-44487

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

2021 (2)

CVE-2021-23817

A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

Exploitability Analysis

Factor	Assessment
Exploit Maturity	Proof-of-Concept available
Attack Prerequisites	Nginx resolver directive must be configured; attacker must influence DNS responses
Skill Level Required	High - Requires DNS infrastructure control or MITM position
Reliability	Medium - Depends on configuration and memory layout
Detectability	Low - May appear as normal DNS traffic

Exploitation Feasibility: MEDIUM-HIGH

Exploitation requires the resolver directive to be active in Nginx configuration. If configured, the vulnerability is exploitable via:

- Compromised upstream DNS servers
- Man-in-the-Middle attacks on DNS traffic
- DNS cache poisoning

Potential Impact:

- **Memory Corruption:** Potential for arbitrary code execution on web server
- **Information Disclosure:** Leakage of sensitive server memory contents
- **Service Disruption:** Nginx worker process crashes
- **Server Compromise:** Complete server takeover if code execution achieved
- **Lateral Movement:** Pivot point for internal network attacks

OWASP Top 10 Mapping:

- A06:2021 - Vulnerable and Outdated Components
- A05:2021 - Security Misconfiguration

Remediation Steps

IMMEDIATE:

- Verify Nginx configuration for resolver directive usage
- If resolver is in use, upgrade Nginx to 1.20.1 or later immediately
- Review DNS infrastructure security controls

Short-Term:

- Implement DNSSEC validation if resolver is required
- Use trusted, hardened internal DNS resolvers only
- Segregate DNS resolution traffic on secure network segments

Long-Term:

- Audit all DNS resolution dependencies across infrastructure
- Implement DNS query logging and anomaly detection
- Consider eliminating dynamic DNS resolution where static configuration is viable

5.4 VULNERABILITY #4: ALPACA Cross-Protocol Attack

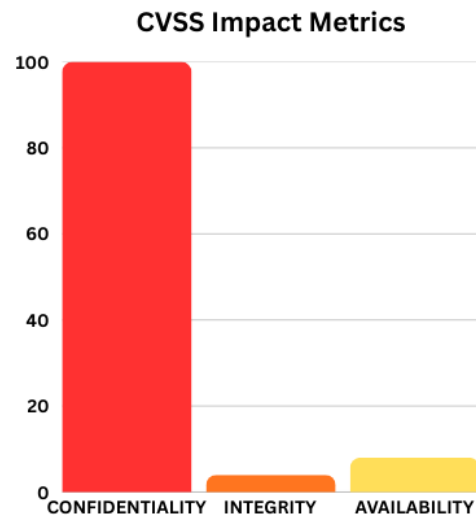
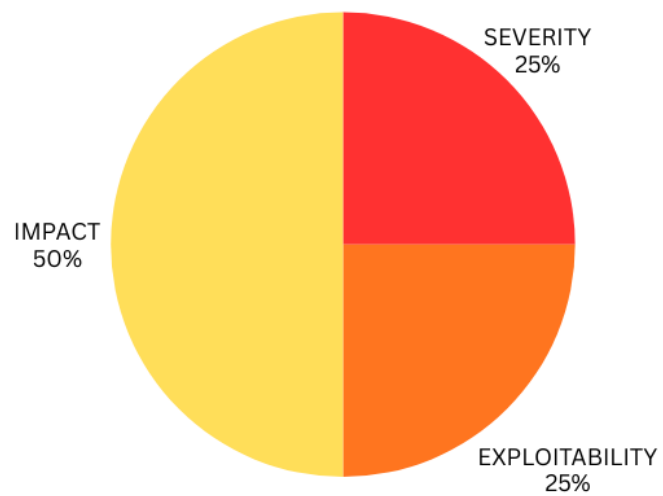
CVE ID	CVE-2021-3618
Vulnerability Name	ALPACA Cross-Protocol Attack
CVSS Score	5.9
Severity	MEDIUM
Exploitability	LOW-MEDIUM
Impact	MEDIUM
OWASP Category	A02:2021 - Cryptographic Failures

CVSS v3.1 Vector Breakdown

Metric	Value	Description
Attack Vector (AV)	Network (N)	Exploitable over network
Attack Complexity (AC)	High (H)	Requires MITM position
Privileges Required (PR)	None (N)	No authentication needed
User Interaction (UI)	None (N)	No user interaction required
Scope (S)	Unchanged (U)	Impact limited to TLS layer
Confidentiality (C)	High (H)	Session confidentiality compromise
Integrity (I)	None (N)	No direct integrity impact
Availability (A)	None (N)	No availability impact

Description:

The ALPACA (Application Layer Protocol Confusion - Analysing and mitigating Cracks in TLS Authentication) attack exploits TLS servers that do not properly enforce application layer protocol restrictions. Attackers in a Man-in-the-Middle position can redirect TLS traffic intended for one protocol (e.g., HTTPS) to another service (e.g., FTP, SMTP) sharing the same certificate, potentially leading to authentication bypass or data leakage.

Security Impact Breakdown:**Evidence**

- Wildcard certificate deployed (.uoc.ac.in)
- Multiple services potentially sharing certificate authority (Inferred)
- Nginx version vulnerable to cross-protocol attacks without proper ALPN enforcement

Proof Of Concept:

General Information	
Country	India
City	Kozhikode
Organization	Calicut University, Kerala
ISP	NKN Core Network
ASN	AS55824
Operating System	Ubuntu
Web Technologies	
Operating Systems	Web Servers
Ubuntu	Nginx 1.18.0
Reverse Proxies	
Nginx 1.18.0	
Vulnerabilities All ports Latest	
Note: the device may not be impacted by all of these issues. The vulnerabilities are impled based on the software and version.	
2025 (1)	
CVE-2025-23419	4.3 When multiple server blocks are configured to share the same IP address and port, an attacker can use session resumption to bypass client certificate authentication requirements on these servers. This vulnerability arises when TLS Session Tickets https://nginx.org/en/docs/http/nginx_http_ssl_module.html#ssl_session_ticket_key are used and/or the SSL session cache https://nginx.org/en/docs/http/nginx_http_ssl_module.html#ssl_session_cache are used in the default server and the default server is performing client certificate authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.
2023 (1)	
CVE-2023-44487	7.5 The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.
2021 (2)	
CVE-2021-23817	7.7 A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.
CVE-2021-3618	7.4 ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MITM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

Exploitability Analysis

Factor	Assessment
Exploit Maturity	Proof-of-Concept demonstrated
Attack Prerequisites	MITM position, multiple services sharing certificate
Skill Level Required	High - Requires network positioning and protocol expertise
Reliability	Low-Medium - Depends on service configuration
Detectability	Very Low - Traffic appears legitimate to target services

Exploitation Feasibility: LOW-MEDIUM

Requires adversary to achieve Man-in-the-Middle position (compromised network, ARP spoofing, or BGP hijacking). Attack complexity is high but impact can be significant if multiple services share wildcard certificates.

Potential Impact:

- **Authentication Bypass:** Cross-protocol authentication token leakage
- **Session Hijacking:** Redirection of authenticated sessions to attacker-controlled services
- **Credential Exposure:** Credentials transmitted to unintended protocol handlers
- **Data Leakage:** Sensitive data exposed through protocol confusion

Impact Scope: Depends on services sharing the wildcard certificate (*.uoc. ac.in)

OWASP Top 10 Mapping

- A02:2021 - Cryptographic Failures
- A05:2021 - Security Misconfiguration

Remediation Steps

IMMEDIATE:

- Audit all services utilizing the *.uoc. ac.in wildcard certificate
- Implement strict ALPN (Application-Layer Protocol Negotiation) enforcement
- Upgrade Nginx to version with enhanced ALPN validation

Short-Term:

- Replace wildcard certificate with service-specific certificates where feasible
- Implement certificate pinning for critical services
- Enable ALPN enforcement in TLS configuration

Long-Term:

- Adopt zero-trust network architecture principles
- Implement mutual TLS (mTLS) for internal service communication
- Deploy network segmentation to isolate protocol-specific services

6. EXPLOITABILITY & RISK MATRIX

6.1 Vulnerability Risk Matrix

Vulnerability	Exploitability	Impact	Overall Risk
CVE-2025-23419 (TLS Auth Bypass)	HIGH	CRITICAL	CRITICAL
CVE-2023-44487 (HTTP/2 Rapid Reset)	VERY HIGH	HIGH	CRITICAL
CVE-2021-23017 (DNS Memory Corruption)	MEDIUM-HIGH	HIGH	HIGH
CVE-2021-3618 (ALPACA)	LOW-MEDIUM	MEDIUM	MEDIUM
Nginx 1.18.0 EOL	N/A	HIGH	CRITICAL

6.2 Technical Risk Rating

Overall Technical Risk: CRITICAL

Justification:

- Multiple critical and high-severity vulnerabilities present
- End-of-life software in production without security support
- Authentication bypass and remote code execution vectors identified
- Denial-of-service attacks readily executable with public tools
- Unknown CMS version introduces additional unquantified risk

6.3 Attack Path Analysis

Most Likely Attack Scenarios:

1. Opportunistic DDoS Attack (Highest Probability)

Exploit: CVE-2023-44487 (HTTP/2 Rapid Reset)

Skill Required: Low

Impact: Service disruption during critical academic periods

2. Authentication Bypass for Data Theft (Highest Impact)

Exploit: CVE-2025-23419 (TLS Session Resumption)

Skill Required: Medium

Impact: Unauthorized access to student/faculty data

3. Server Compromise via Memory Corruption (Conditional)

Exploit: CVE-2021-23017 (DNS Resolver)

Skill Required: High

Impact: Complete server takeover if DNS resolver is configured

7. CONCLUSION & REMEDIATION

7.1 Summary of Critical Risks

The University of Calicut's web infrastructure exhibits **critical security deficiencies** requiring immediate attention:

End-of-Life Software: Nginx 1.18.0 has not received security updates for nearly 5 years

Authentication Vulnerabilities: Critical TLS session resumption bypass (CVE-2025-23419)

Availability Threats: HTTP/2 Rapid Reset vulnerability enables easy DDoS attacks

The combination of these factors creates a **high-probability, high-impact threat scenario** that could result in:

- Unauthorized access to sensitive educational data
- Service disruptions affecting academic operations
- Potential regulatory compliance violations
- Institutional reputation damage

7.2 Immediate Actions - CRITICAL PRIORITY

Action	Priority	Effort	Impact
Upgrade Nginx to 1.24.x or 1.25.x	P0	Medium	Critical
Identify and patch Joomla version	P0	Low	High
Implement HTTP/2 rate limiting	P0	Low	High
Verify DNS resolver configuration	P1	Low	Medium
Deploy temporary WAF rules	P1	Medium	Medium
Enable enhanced security logging	P1	Low	Medium

Detailed Immediate Actions:

1. Nginx Upgrade

- Test upgrade in staging environment
- Schedule maintenance window
- Upgrade production to Nginx 1.24.0 or later
- Verify all CVEs are patched post-upgrade

2. DDoS Mitigation

- Implement HTTP/2 connection and stream limits
- Deploy rate limiting at application and network layers
- Engage DDoS mitigation service provider (Cloudflare, Akamai)

7.3 Short-Term Actions

Action	Priority	Effort	Impact
Implement Web Application Firewall	P1	High	High
Deploy certificate management strategy	P2	Medium	Medium
Establish vulnerability scanning program	P1	Medium	High
Conduct authenticated application assessment	P1	Medium	High
Implement SIEM for security monitoring	P2	High	Medium
Review and harden PHP configuration	P2	Low	Medium

Detailed Short-Term Actions:

1. Web Application Firewall Deployment

- Deploy MoD Security or cloud-based WAF
- Configure OWASP Core Rule Set (CRS)
- Implement Joomla-specific protections
- Enable virtual patching for known vulnerabilities

2. Vulnerability Management Program

- Implement automated vulnerability scanning (Nessus, Qualys, OpenVAS)
- Schedule monthly external and internal scans
- Establish SLA for vulnerability remediation by severity
- Create vulnerability tracking and reporting procedures

3. Application Security Assessment

- Conduct authenticated Joomla security audit
- Perform OWASP Top 10 testing
- Review custom code for vulnerabilities
- Assess administrative access controls

7.4 Long-Term Security Improvements

Strategic Security Initiatives:

1. Infrastructure Modernization

- Migrate to container-based architecture (Docker/Kubernetes)
- Implement Infrastructure as Code (IaC) for configuration management
- Adopt DevSecOps practices with security integrated into CI/CD pipelines

2. Security Architecture Enhancements

- Deploy zero-trust network architecture
- Implement micro-segmentation for service isolation
- Deploy mutual TLS (mTLS) for service-to-service communication
- Establish defence-in-depth security controls

3. Governance and Compliance

- Develop formal Information Security Policy
- Implement Security Patch Management Policy with defined SLAs
- Establish Change Management procedures for production systems
- Create Incident Response and Disaster Recovery plans
- Conduct annual third-party security audits

4. Security Operations

- Establish Security Operations Centre (SOC) or outsource to MSSP
- Implement Security Information and Event Management (SIEM)
- Deploy Intrusion Detection/Prevention Systems (IDS/IPS)
- Establish threat intelligence program
- Conduct regular penetration testing (annual minimum)

5. Education and Awareness

- Implement security awareness training for IT staff
- Establish secure development training for developers
- Create security incident reporting procedures
- Conduct tabletop exercises for incident response

8. REFERENCES

8.1 CVE References

CVE-2025-23419 - Nginx TLS Session Resumption Authentication Bypass <https://nvd.nist.gov/vuln/detail/CVE-2025-23419>

CVE-2023-44487 - HTTP/2 Rapid Reset Denial of Service <https://nvd.nist.gov/vuln/detail/CVE-2023-44487>
<https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487>

CVE-2021-23017 - Nginx DNS Resolver 1-Byte Memory Overwrite
<https://nvd.nist.gov/vuln/detail/CVE-2021-23017>
https://nginx.org/en/security_advisories.html

CVE-2021-3618 - ALPACA TLS Cross-Protocol Attack
<https://nvd.nist.gov/vuln/detail/CVE-2021-3618> <https://alpaca-attack.com/>

8.2 OWASP Resources

OWASP Top 10 (2021)
<https://owasp.org/www-project-top-ten/>

OWASP Web Security Testing Guide
<https://owasp.org/www-project-web-security-testing-guide/>

OWASP ModSecurity Core Rule Set
<https://owasp.org/www-project-modsecurity-core-rule-set/>

8.3 Vendor Security Advisories

Nginx Security Advisories
https://nginx.org/en/security_advisories.html

Nginx Changelog and Version History
<https://nginx.org/en/CHANGES>

Ubuntu Security Notices
<https://ubuntu.com/security/notices>