eScan Security Advisory Creation Date: January 22, 2026
Last updated date: January 27, 2026
Current Operational Risk: Medium (contained, mitigated)
Vector Severity: High
Overall Assessment: Medium-High
Status: Resolved
Advisory ID: ESCAN-2026-001

## Executive Summary

eScan experienced a temporary update service disruption starting January 20, 2026, affecting a subset of customers whose systems automatically download updates during a specific timeframe, from a specific update cluster. The issue resulted from unauthorized access to regional update server infrastructure. The incident has been identified and resolved. Comprehensive remediation is available that addresses all observed scenarios.

## What Happened

### Incident Description

Unauthorized access to one of our regional update server configurations resulted in an incorrect file (patch configuration binary/corrupt update) being placed in the update distribution path. This file was distributed to customers downloading updates from the affected server cluster during a limited timeframe on January 20, 2026.

**Important Clarification:** The file distributed was **not an official eScan binary or update**.

### Affected Distribution Details

- **Date:** January 20, 2026
- **Time Window:** Limited period (approximately 2 hours)
- **Deployment Channel:** Single regional update server cluster
- **File Status:** Unauthorized file (NOT an official eScan release)

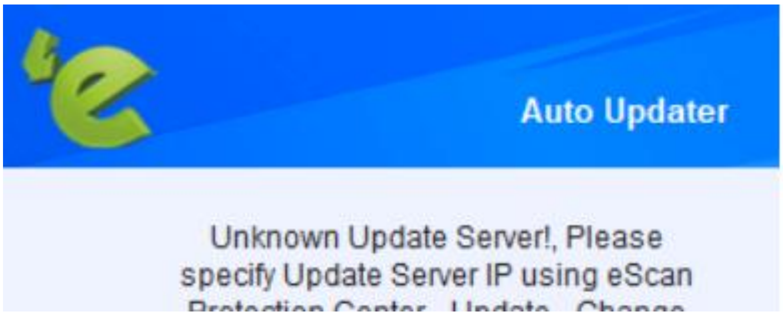
## Customer Impact and Risk Assessment

### Affected Systems

Customers who downloaded eScan updates starting January 20, 2026, from the affected regional server cluster may have experienced:

**Primary Indicators:**

- Update service failure notifications
- Modified system hosts file preventing connection to eScan update servers
- eScan update configuration file modifications
- Inability to receive new security definition updates
- Update unavailability popup on client machines



Unknown Update Server!, Please specify Update Server IP using eScan Protection Center - Update - Change

**Impact Levels:**

- Enterprise: Medium-High
- Consumer: Low-Medium

**System Scope:**

- **Operating Systems:** Windows-based endpoints (all versions)
- **Affected Category:** Limited number of customers in specific geographic regions from a specific update cluster during the incident timeframe

**NOT Affected**

- eScan product code (no product defect or vulnerability)
- Customers who did not download updates during incident window
- Customers routing through other regional update servers
- Core eScan protection capabilities continue operating normally

## Incident Classification

**Nature of Incident – Root Cause Analysis**

**This was an infrastructure service disruption incident, NOT a product defect.**

**Specifically:**

- Update infrastructure access incident: **YES**
- Unauthorized patch misconfiguration file: **YES**
- eScan product vulnerability: **NO**
- Faulty legitimate patch: **NO**

The incident affected update distribution infrastructure only. There is no vulnerability in eScan product software itself. eScan's core endpoint protection, threat detection, and security features continue to operate normally and effectively.

---

## What eScan Did

**Immediate Response Actions – Containment and Remediation**

1. **Rapid Detection & Isolation**
   - Incident detected through customer reports and internal monitoring
   - Affected update infrastructure isolated within 2 hours
2. **Precautionary Infrastructure Validation**
   - Temporarily took global update infrastructure offline for comprehensive validation
   - Ensured no other systems affected
3. **Comprehensive Investigation**
   - Conducted thorough analysis to identify all affected components
   - Analyzed system impacts across affected customer base
   - Developed complete remediation approach
4. **Remediation Development & Deployment**
   - Created remediation tool addressing all scenarios
   - Tested thoroughly before deployment

5. **Infrastructure Hardening**
    - Rebuilt affected infrastructure with enhanced security
    - Implemented additional security controls and monitoring
    - Enhanced access controls and authentication requirements

## Current Status

### Resolution Status

- Affected infrastructure isolated and rebuilt with enhanced security
- All authentication credentials rotated globally
- Comprehensive remediation available and deployed to affected customers
- Enhanced monitoring and security controls implemented across all infrastructure
- Update services operating normally with strengthened protections
- Ongoing verification and customer support active

### Enhanced Security Measures

**Access Security:**

- Enhanced credential rotation policies
- Additional access control validation layers

**Infrastructure Protection:**

- Real-time file integrity monitoring on update servers
- Enhanced change detection and alerting
- Automated validation of update authenticity
- Improved change management controls

**Operational Improvements:**

- Improved incident response procedures
- Customer notification protocol enhancements

## What Customers Should Do – Support and Accountability

**If You Experienced Update Issues Starting January 20:**

**Immediate Action Required:**

1. **Contact eScan Support Immediately:**
   - **Email:** support@escanav.com
   - **Online Chat:** https://escanav.com/livechat
   - **Phone:** 18002672900/0091-22-67722911
2. **Our Support Team Will:**
   - Verify if your system was affected
   - Provide comprehensive remediation update
   - Conduct remote verification session
   - Confirm successful restoration of all services
3. **Important:** In most cases, customers need to download and manually run the below patch and apply on individual systems.

## Remediation Process

**What the Remediation Update Does:**

- Automatically identifies and corrects incorrect modifications
- Re-enables proper eScan update functionality
- Verifies successful restoration
- Requires standard system restart

**Verification Confirmation:** After remediation, you should observe:

- eScan update services resume normal operation
- No error popups or update failure messages
- Latest security definitions downloading successfully
- All eScan protection features operating normally

**If You Did NOT Experience Any Update Issues:**

- No action required
- Your system was not affected by this incident
- eScan continues to provide normal protection
- Safe to continue receiving eScan updates

---

## Additional Information

**Update Service Safety**

**Current Update Infrastructure Status:**

- All update infrastructure validated and secure
- Enhanced monitoring and controls active
- Safe to continue receiving eScan updates
- No need to disable updates or isolate endpoints

**Network-Level Protection**

For additional precautionary measures, organizations must implement firewall blocks for:

- vhs.delrosal.net
- tumama.hns.to
- 504e1a42.host.njalla.net
- 185.241.208.115

*Note: Not required for systems that have received remediation.*

## Technical Support Availability

**Dedicated Support for This Incident:**

- 24/7 support availability for affected customers
- Priority handling for all incident-related inquiries
- Direct escalation paths available
- Commitment to complete resolution and verification

---

## Frequently Asked Questions

**Q: Was this a security attack?**

A: This was an infrastructure access incident affecting our update distribution system. The eScan product itself contains no vulnerability.

**Q: Is my data at risk?**

A: No customer data was accessed or affected. The incident impacted update distribution infrastructure only.

**Q: Do I need to uninstall and reinstall eScan?**

A: No. Our automated remediation update addresses all modifications. No uninstall/reinstall required.

**Q: Can I trust eScan updates now?**

A: Yes. The incident has been resolved, infrastructure rebuilt with enhanced security, and additional controls implemented to prevent recurrence.

**Q: Why wasn't I notified proactively?**

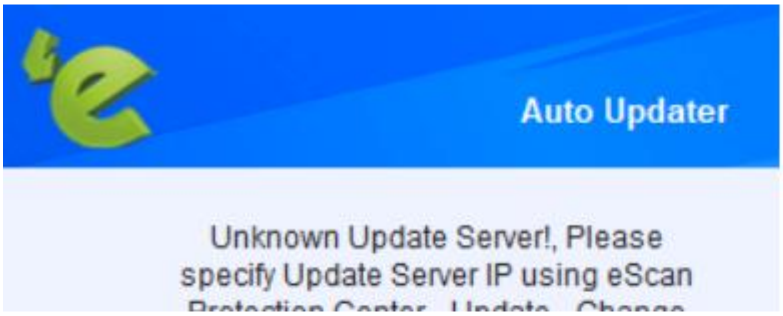
A: Our response focused on providing immediate verified remediation to affected customers through direct support channels. We are reviewing our incident communication protocols as part of continuous improvement.

**Q: Will this happen again?**

A: We have implemented comprehensive preventive controls including enhanced authentication, real-time monitoring, automated validation, and additional security layers to prevent recurrence.

**Q: Which customer should connect to eScan Technical support?**

A: Customers facing the below pop-up should connect to eScan Technical support for further assistance.



Unknown Update Server!, Please specify Update Server IP using eScan Protection Center - Update - Change

## Commitment to Transparency

We are committed to maintaining the highest security standards for our infrastructure and appreciate your continued trust in eScan.

This advisory will be updated if additional information becomes available.

Technical advisory will be available shortly.

## Contact Information

**For Technical Support:**

- **Email:** support@escanav.com
- **Online Support:** https://escanav.com/livechat
- **Phone:** 18002672900/0091-22-67722911

**For Security Inquiries:**

- **Email:** security@escanav.com

**For Enterprise Customers:**

- **Dedicated Support:** 0091-99209 07188/0091-98692 58689/0091-95940 02570
- **Email:** corpsupport@escanav.com

**Executive Escalation:**

Available through support channels for critical issues.