**Information Security Audit Report LDIL.DE**

Group A

Group Assignment

January 2018

Technology, communication and transport

Cyber Security

|  |  |  |
| --- | --- | --- |
| jamk_fi_tunnus_sininen | | **Description** |
| Author(s)  Jani Lindholm  Otso Korpelainen  Vesa Simola  Pauli Paatsola  Pinja Koskinen  Petri Toropainen  Teemu Hokkanen  Jouni Ihanus  Janne Ahokas  Otso Korpela  Jani Lindholm | Type of publication  Group Assignment | Date January 2018 |
| Language of publication: |
| Number of pages | Permission for web publication: x | |
| Title of publication  **Group Assignment: Information Security Audit Report for LDIL.DE** | | |
| Degree programme  Master’s Degree Programme in Information Technology | | |
| Supervisor(s)  Lötjönen, Jarmo | | |
| Assigned by  Lötjönen, Jarmo | | |
| Abstract  This document presents information security audit report for LDIL.DE. Assignment is part of auditing and testing technical security course.  The main reference framework used in this audit is Payment Card Industry Data Security Standard (PCI DSS). Also, some part outside this framework is presented as required in assignment.  Document walks through accomplished audit activities and main findings, ending with recommendations and detailed technical report. Full reports produced by auditing tools are included as attachment.  Conclusion is that technical environment does not fully comply with PCI DSS. The management should take in to consideration findings presented in this document as part of the risk management activities. Recommendations should be prioritized and responsibilities should be defined. | | |
| Keywords/tags ([subjects](https://janet.finna.fi/Search/Results?lookfor=asiasanastot&prefiltered=format_Database&SearchForm_submit=Find&retainFilters=0&filter%5b%5d=format%3A%220%2FDatabase%2F%22&lng=en-gb))  Security, Audit, NMAP, Nessus, OWASP | | |
| Miscellaneous ([Confidential information](https://intra.jamk.fi/opiskelijat/student/thesis/Pages/publicity.aspx)) | | |

Table of Contents

[1 Introduction 1](#_Toc503125984)

[2 Target organization 1](#_Toc503125985)

[3 Scope of the audit 1](#_Toc503125986)

[4 Audit activities 2](#_Toc503125987)

[4.1 Publicly available networks (DMZ, etc.) 3](#_Toc503125988)

[4.2 Workstation network and WEB testing (Internal and branch) 3](#_Toc503125989)

[4.3 Management networks (MGMT, warehouse and staff) 4](#_Toc503125990)

[5 Main findings 4](#_Toc503125991)

[5.1 Publicly available networks (DMZ, etc.) 5](#_Toc503125992)

[5.2 Workstation network (Internal and branch) 5](#_Toc503125993)

[5.3 Management networks (MGMT, warehouse and staff) 5](#_Toc503125994)

[6 Recommendations 6](#_Toc503125995)

[7 Detailed Technical Report 6](#_Toc503125996)

[7.1 Tooling 6](#_Toc503125997)

[7.2 Executed Test Cases 7](#_Toc503125998)

[7.3 Vulnerability Summary 7](#_Toc503125999)

[7.4 Vulnerability Details 11](#_Toc503126000)

[8 Sample Report – Attachments 20](#_Toc503126001)

Figures

**No table of figures entries found.**

Tables

[Table 1 Tools and versions used. 6](#_Toc503126002)

[Table 2 Executed test cases 7](#_Toc503126003)

[Table 3 DMZ internal vulnerabilities summary 8](#_Toc503126004)

[Table 4 DMZ and external vulnerabilities summary 8](#_Toc503126005)

[Table 5 Internal services vulnerabilities summary 9](#_Toc503126006)

[Table 6 Branch vulnerabilities summary 10](#_Toc503126007)

[Table 7 Management network vulnerabilities summary 11](#_Toc503126008)

[Table 8 Warehouse vulnerabilities summary 11](#_Toc503126009)

[Table 9 Attachment files 21](#_Toc503126010)

# Introduction

This auditing report is a group exercise and it is part of the Auditing and Testing Technical Security course. Report includes external and internal network security tests performed against the LDIL corporate network. The goal of the technical security audit is to form overall picture relating to state of the security and offer recommendations for future improvements.

# Target organization

LDIL is a national e-tailing company that also has one physical retail store with a POS-system. LDIL business environment consists of information systems and different network domains. Target of this evaluation is LDIL's systems and networks related to customer and payment information.

# Scope of the audit

The reference framework used in this audit is Payment Card Industry Data Security Standard (PCI DSS). Based on this framework, all components that are part of cardholder data environment should be included to the scope of audit. Also, as assignment required, all other component that were available for testing were included. Even so, reference framework was required to transform priority rating for different systems to support audit priorities (findings, recommendations, etc.).

As a notice, it should be reminded that this audit is purely technical and do not include any administrative parts relating to used framework.

From technical perspective audit can also be divided to internal and external audit as presented below:

* **Internal audit** was performed inside LDIL’s network. Detailed information about network structure and host credentials were available for deep inspection.
* **External audit** was performed against LDIL’s publicly available network interface.

Detailed scope of technical functions (networks, etc.) is presented in next chapter.

# Audit activities

Three subgroups were created from group A auditing personnel and each group was assigned part of the LDIL network segments to perform the audit. The auditing groups were formed to most effectively utilize the assessor’s skills. Petri and Jouni were chosen as lead auditors to facilitate the auditing process.

Groups were following:

* Vesa & Pinja (Publicly available networks)
* Pauli, Jani, Otso & Janne (Workstation network and WEB testing)
* Jouni, Teemu & Petri (Management networks)

Network segments to be audited were divided based on workload estimates and by logical entities.

Internal auditing activities were conducted by using virtualized Kali workstations and tools installed on them. These workstations had interfaces on all relevant network segments. External auditing activities were conducted by using RGCE internet workstation located outside of the LDIL network perimeter and RGCE Nessus service.

LDIL firewall rules (Palo Alto and pfsense) were reviewed to find possible shortcomings.

Used review techniques in this audit can be divided in two parts:

* Passive techniques
  + Documentation review
  + Ruleset review (Firewall)
* Active techniques
  + Network discovery
  + Network port and service identification
  + Vulnerability scanning

There were small differences in used techniques and activities based on what kind of functions were under inspection. These details are presented in next chapters.

## Publicly available networks (DMZ, etc.)

Premilinary scanning of the public address space and 1:1 NAT inside network was performed using Nessus vulnerability scanner and Nmap port scanner. Two aforementioned tools were used from both inside and outside of the perimeter firewall. First order of business was running Nmap and Nessus was used to both confirm the Nmap findings and to scan for higher level vulnerabilities. Reports produced by the automated scanners were analyzed manually to find the most relevant issues that were deemed worthy of escalation. Masses of bulk vulnerabilities that were found were intentionally left out as they could have been trivially patched assuming patches where available in RGCE. These are still reported in the attachments.

Hence, we selected a few of the more critical and subject-wise interesting vulnerabilities, for example: Shellshock and weak encryption mechanisms. These are discussed in more detail from the ldil.de perspective with PCI DSS angle.

## Workstation network and WEB testing (Internal and branch)

Internal and Branch networks included the following network segments:

* Internal 10.0.100.1/24
* Branch 192.168.10.1/24

Web testing was conducted to corresponding web-services found in internal-branch-servers.  
Focus of web testing was to discover application flaws or misconfigurations. Web testing revealed certain issues regarding the used libraries, operating system and applications. Verbose error http responses are spreading out too much information about the target machines, e.g. stating the version of PHP, OS and Apache.  
  
Threats regarding the application were discovered by either manually testing or automatically scanning the target machines with Owasp ZAP and Nessus.

We were comparing the regarding the vulnerability scanning, by evaluating both Nessus and OpenVAS - but we ended up using Nessus because of company policy, other participants in the conducted audit were also using the Nessus.

More detailed issue reports can be found on chapter 7. In addition to verbose http responses or error messages, there were also buffer overflows, misconfigured application/server issues found.

## Management networks (MGMT, warehouse and staff)

Management networks included the following network segments:

* MGMT 10.99.0.1/24
* Warehouse 172.20.0.0/24
* Staff-we 10.10.0.0/24
* Branch-staff 192.168.20.0/24

From the PCI DSS point of view, especially MGMT-segment is critical. Most of the management devices are located in this network segment as well as log servers just to mention a few. In order to ensure the security of CPE environment, these can be seen as critical components.

Auditing were conducted first by running a Nessus discovery scan to discover all connected hosts in all the segments. Results from this scan were compared to the LDIL service catalog provided by LDIL personnel. After determining host’s operating systems and that no unrecognized hosts were not found, a new and more specific Nessus scans were conducted to acquire more information about the systems. Some findings were verified by using OpenVAS tool.

# Main findings

* Segmentti kohtaiset kriittisimmät huomiot palveluihin liittyen
* Muistetaan PCI DSS näkökulma

Based on their auditing findings each subgroup presented main findings and summary of these findings is presented here.

Firewall rule

* Yksi näkökulma: Verrattuna siihen olemassa olevaan dokumentaation (asiakkaan luovuttamaa)

## Publicly available networks (DMZ, etc.)

General consensus is that the majority of the vulnerabilities found during our scanning of both the inside and outside address spaces of the 1:1 NAT were a result of missing software updates on the relevant servers.

Now, the reason for this most likely is that there simply was no updates available in the RGCE mirrors, hence we've decided to skip the low hanging fruits this scenario proposed and instead we attempted to come up with some less obvious findings and discuss few of the critical flaws found in more detail, that being said, in more general level concerning the given well known vulnerabilities.

### Issues with the port scanning

We attempted to port scan the whole subnet using various NMAP switches. But during our testing we witnessed some strange behavior on the ldil.de firewall. Next is a brief description of the open ports detected and the aforementioned behavior of interest. Nevertheless, we got some results in overall, after combining the results achieved from the Nessus scan and partial results of NMAP scans. Under the topic "Vulnerability findings found from outside the perimeter firewall" we will depict the results achieved from the scanning executed from outside the firewall.

## Workstation network (Internal and branch)

Based on information gathered during the auditing activities most of the systems were poorly updated and therefore many security vulnerabilities were found.

We detected some critical vulnerabilities in Windows SMB-service and DNS-service of multiple servers. Those vulnerabilities allow remote code execution in the server or allow those servers to be used in a denial of service attack. Also, support to weak algorithms is enabled in SSH-server.

## Management networks (MGMT, warehouse and staff)

Based on information gathered during the auditing activities most of the systems were poorly updated and therefore many security vulnerabilities were found.

# Recommendations

* Edellä kuvattuihin kriittisiin havaintoihin liittyvät prioriteetit
  + Arvioidaan PCI DSS näkökulmasta
  + ”Yhteenveto”
    - Ei vastaa PCI DSS
    - Suositellaan korjattavaksi
    - Vastuutetaan ja aikataulutetaan

In general, the first and foremost task or activity that should take place based on the results of this audit would be to upgrade the software components of the given target systems. This is essential as it would cover majority of vulnerabilities found in systematic and logical manner. To accomplish this, software repositories need updating and possibly reconfiguration.

As with any software upgrade, this task should be split and prioritized so that the most impactful systems are patched first. Yet, to do this in safe and mature manner this patching should be done in pre-production or testing environment before touching the production system. This is key in order to avoid causing mayhem on the production that could occure due to broken software packages or incompabilities introduced by version changes.

Some of the found vulnerabilities are more complex and require configuration changes in addition to software upgrade. Example of this kind of vulnerability would be the weak encryption algorithms. To fix these in safe manner it would be ideal to first check that also the surrounding software stack supports the stonger, more modern, encryption methods.

All in all, the key take away from this report is that the software is largely outdated and needs actions to be taken.

Fix update process to keep everything updated and fix firewall rules.

Disable old encryption protocols and update encryption software to newest version.

# Detailed Technical Report

Group A technical security testers were utilized to test and audit the LDIL corporate network thoroughly. Throughout the testing process, set of tools and preplanned test cases are planned - based on use cases given on LDIL business logic. The architecture of the LDIL is known as well as LDIL personnel are aware that audit and testing is performed to the corporate system. The testing type lies between crystal and grey-box combination - mainly testing the tester’s effectiveness and also the vulnerabilities on outdated system.

## Tooling

The following tools listed in table 1 were used to conduct the security assessment. The tools are divided into information gathering, vulnerability scanning and also on web testing.

Table 1 Tools and versions used.

|  |  |
| --- | --- |
| Tools and version | |
| Nmap | 6.40 |
| Nessus | 5.9 |
| Openvas |  |
| Burp Suite | 1.7.03 |
| Owasp ZAP | 2.7.0 |

## Executed Test Cases

Table 2 contains a list of tests that were conducted during the test. This table does not contain any indication whether or not the test found any vulnerabilities. Summary of detected vulnerabilities are listed in section 7.5.

Apart from the detailed test cases, also exploratory testing was applied by using Burp suite and Owasp ZAP.

Table 2 Executed test cases

|  |  |
| --- | --- |
| Test Cases | |
| Executed tests provided by Nmap | Port and service enumeration scan. |
| Executed tests provided by Nessus | Vulnerability scan |
| Executed tests provided by OpenVas | Vulnerability scan |
| Burp Suite / Owasp ZAP | Web application testing, penetration testing |

## Vulnerability Summary

The purpose of this chapter is to gather an executive summary of all the findings so that it’s possible to get a fast general understanding of the state of the cyber security in the Ldil network. (The hosts .222, .234, and .237 for Kali and .251 for Nessus in each network segment are not included in the summary.) Each network segment is detailed separately. The unknown or undocumented services are at the end, otherwise all the host are in ascending order by their IP address.

### DMZ vulnerability summary

Internally the services in DMZ contain several vulnerabilities. The most secure service, after the firewall, is the Mail server. Others have several critical and high-risk vulnerabilities. There should be limited access to the internal network segments, but even so, for example the compromise of web-server might prevent the customers from accessing the site and thus hinder the money flow from customers. The internal vulnerabilities are summarized in the table 3. The external, or Internet facing services or addresses, are in the table 4. There is nothing alerting in the Internet facing services.

Table 3 DMZ internal vulnerabilities summary

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Host** | **Service** | **Critical** | **High** | **Med** | **Low** | **Info** |
| 10.10.10.1 | Firewall | 0 | 0 | 0 | 0 | 3 |
| 10.10.10.4 | ns1 | 16 | 89 | 101 | 7 | 38 |
| 10.10.10.7 | Unknown | 0 | 0 | 0 | 0 | 9 |
| 10.10.10.8 | ns2 | 16 | 89 | 101 | 7 | 38 |
| 10.10.10.10 | extranet | 19 | 90 | 131 | 9 | 60 |
| 10.10.10.20 | www | 22 | 95 | 136 | 12 | 69 |
| 10.10.10.30 | Mail | 0 | 0 | 11 | 9 | 54 |
| 10.10.10.40 | Helpdesk | 19 | 95 | 124 | 7 | 35 |

Table 4 DMZ and external vulnerabilities summary

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Host** | **Service** | **Critical** | **High** | **Med** | **Low** | **Info** |
| 60.254.143.2 | Carrier PE | 0 | 0 | 0 | 0 | 8 |
| 60.254.143.2 | Branch FW | 0 | 0 | 3 | 0 | 0 |
| 79.99.193.10 | Extranet.ldil.de | 0 | 0 | 0 | 0 | 4 |
| 79.99.193.20 | [www.ldil.de](http://www.ldil.de) | 0 | 0 | 0 | 0 | 4 |

### Internal and Branch vulnerabilities summary

Internal services contain the Domain Controller for Windows workstations, Fileserver, Intranet and MySQL –database. The two latter ones have 19 critical vulnerabilities and almost a hundred high-risk vulnerabilities each. Through the intranet the malicious actor could have access to all the workstations that access the Intranet. Compromising MySQL –server on the other hand may cause irreparable damage to the database. Also, there was again one host, .91, of which we couldn’t find from the service catalog. Again, in the Ldil Cyber Security Implementation report mentions about the Apache server being setup and left un-updated. The summary of the vulnerabilities found in the services is in the table 5.

Table 5 Internal services vulnerabilities summary

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Host** | **Service** | **Critical** | **High** | **Med** | **Low** | **Info** |
| 10.99.0.1 | Firewall | 0 | 1 | 8 | 2 | 29 |
| 10.99.0.10 | Log1 | 12 | 49 | 52 | 8 | 49 |
| 10.99.0.11 | Log2 | 11 | 49 | 52 | 8 | 49 |
| 10.99.0.110 | FSPM | 10 | 144 | 32 | 2 | 94 |
| 10.99.0.120 | PRTG | 1 | 0 | 4 | 0 | 23 |
| 10.99.0.130 | CCTV-Manager | 0 | 0 | 3 | 2 | 27 |
| 10.99.0.20 | **Sentinel(?)** | 1 | 0 | 7 | 3 | 35 |
| 10.99.0.21 | **Sentinel** | 0 | 0 | 7 | 3 | 39 |
| 10.99.0.100 | **unknown/mgm** | 0 | 0 | 9 | 2 | 25 |
| 10.99.0.101 | **unknown/mgm** | 0 | 0 | 9 | 2 | 26 |
| 10.99.0.102 | **unknown/mgm** | 1 | 0 | 10 | 3 | 25 |
| 10.99.0.103 | **unknown** | 0 | 0 | 0 | 3 | 3 |
| 10.99.0.104 | **unknown/mgm** | 0 | 0 | 9 | 2 | 25 |
| 10.99.0.105 | **unknown/mgm** | 1 | 0 | 10 | 2 | 25 |
| 10.99.0.106 | **unknown** | 0 | 0 | 9 | 3 | 22 |
| 10.99.0.107 | **unknown** | 0 | 0 | 9 | 2 | 22 |
| 10.99.0.108 | **unknown** | 0 | 0 | 9 | 2 | 22 |
| 10.99.0.109 | **unknown/mgm** | 2 | 0 | 11 | 2 | 34 |
| 10.99.0.111 | **unknown/mgm** | 1 | 0 | 10 | 2 | 25 |

### Branch store segment vulnerabilities summary

In the branch store network segment the only critical vulnerabilities, three in total, were on the read only copy of the Domain Controller. There were no high-risk vulnerabilities in any service.

There was, however, a host that wasn’t catalogued that should be checked, but the best estimate is that it’s an instance of Kali. The summary of the number of vulnerabilities in the branch store segment can be found from the table 6.

Table 6 Branch vulnerabilities summary

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Host** | **Service** | **Critical** | **High** | **Med** | **Low** | **Info** |
| 192.168.10.10 | DC | 3 | 0 | 1 | 0 | 30 |
| 192.168.10.20 | POS | 0 | 0 | 3 | 2 | 31 |
| 192.168.10.30 | InfoTV | 0 | 0 | 0 | 0 | 4 |
| 192.168.10.51 | CCTV-Branch1 | 0 | 0 | 2 | 0 | 18 |
| 192.168.10.52 | CCTV-Branch1 | 0 | 0 | 1 | 0 | 18 |

### Management networks vulnerabilities summary

Management network is one of the most critical network segments, since it contains the Log servers, F-Secure Policy Manager and apparently a cluster of management workstations which are, however, undocumented. The computers running logging services and the F-Secure Policy manager have again several critical and in the case of FSPM, more than hundred high-risk vulnerabilities.

The suspected management computers were identified by their DNS or netbios –name, which contains the string k#### (# representing a number). Those have been labeled with “unknown/mgm” in the table 7 below. The hosts .106-.108 are most likely similar management computers, even though the before mentioned string wasn’t found.

On top of the management computers, the hosts .20 and .21, containing Linux, are undocumented in the service catalog. The .20 most likely contains the NetIQ Sentinel based on the hostname and that is documented in the Ldil’s Cyber Security Implementation report. The .21 is the interface for delivering data for the Sentinel.

Of the host .103 no information was found. All the information is summarized in the table 7.

Table 7 Management network vulnerabilities summary

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Host** | **Service** | **Critical** | **High** | **Med** | **Low** | **Info** |
| 10.99.0.1 | Firewall | 0 | 1 | 8 | 2 | 29 |
| 10.99.0.10 | Log1 | 12 | 49 | 52 | 8 | 49 |
| 10.99.0.11 | Log2 | 11 | 49 | 52 | 8 | 49 |
| 10.99.0.110 | FSPM | 10 | 144 | 32 | 2 | 94 |
| 10.99.0.120 | PRTG | 1 | 0 | 4 | 0 | 23 |
| 10.99.0.130 | CCTV-Manager | 0 | 0 | 3 | 2 | 27 |

### Warehouse network vulnerabilities summary

The warehouse network segment contains the hosts for running services for Human Resources and Front Accounting. The system running the HR services is again extremely vulnerable, with 19 critical and 90 high-risk vulnerabilities. The summary of the vulnerabilities can be found from the table 8.

Table 8 Warehouse vulnerabilities summary

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Host** | **Service** | **Critical** | **High** | **Med** | **Low** | **Info** |
| 172.20.0.10 | HR | 19 | 90 | 126 | 9 | 52 |
| 172.20.0.20 | Front Accounting | 0 | 0 | 0 | 0 | 13 |

## Vulnerability Details

Objective of this title is to issue more technical and detailed information about the most important vulnerabilities presented above. In addition to technical explanation and possible mitigation proposal, overview includes severity and risk assessment to support decision making.

Information is divided based on group responsibilities presented in title four. Full technical records regarding all audit activities are attached to this document.

### List of vulnerabilities in DMZ

|  |
| --- |
| BGP port open  **Synopsis:** BGP control plane possibly vulnerable  **Vulnerable Targets:**  79.99.192.1. According to the documentation, this is the RGCE ISP.  **Vulnerability Explanation:** There is a possible configuration error in form of BGP tcp/179 being reachable from our Nessus scanner. Danger in this configuration is that BGP port is a sign of possibly lacking control plane protections on the ISP router. Possible exploitation vectors include things such as sending RST packet from falsified source address and general overloading of the BGP process on the listening party. Net effect of this is that the would-be BGP peering might be prone to denial of service attacks, given that there is no peerings configured, theBGP tcp/179 should not be open to begin with. Hence, as an exception to the previously mentioned lack of recommended fixes we'd like to point out the following: Assuming that the open BGP port is for future use cases we would like to propose the following mitigation methods.   1. Filter inbound packets based on TTL value - this could be done on both ends of the BGP peering 2. Make sure that the uRPF filters are utilized on both the ISP network in general and in the customer peerings |

### List of vulnerabilities in workstation networks and WEB services

|  |
| --- |
| Vulnerability in DNS Resolution  **Synopsis:** Arbitrary code can be executed on the remote host through the installed Windows DNS client.  **Vulnerable Targets:**  [files.ldil.de](http://files.ldil.de) / 10.0.100.20  [dc.ldil.de](http://dc.ldil.de) / 10.0.100.10  rodc.ldil.de / 192.168.10.10  **Vulnerability Explanation**: A flaw in the way the installed Windows DNS client processes Link-local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account. On Windows Vista, 2008, 7, and 2008 R2, the issue can be exploited remotely.  **Vulnerability Fix**: Install patch for Windows 2008 R2.  **Severity: CRITICAL** |

|  |
| --- |
| Microsoft Windows SMB Server vulnerabilities  **Synopsis:** Multiple vulnerabilities in Microsoft Server Message Block 1.0 (SMBv1)  **Vulnerable Targets:**  [dc.ldil.de](http://dc.ldil.de) / 10.0.100.10  [files.ldil.de](http://files.ldil.de) / 10.0.100.20  rodc.ldil.de / 192.168.10.10  **Vulnerability Explanation**: Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. Exploiting vulnerability is possible for unauthenticated attacker via specially crafted packet, to achieve arbitrary code execution. Related vulnerabilities in National Vulnerability Database: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148.  Also, an information disclosure vulnerability exists in SMB. Exploiting vulnerability is possible for unauthenticated attacker via specially crafted packet, to disclose sensitive information. Related vulnerability in NVD: CVE-2017-0147  In addition, SMB vulnerabilities exist that are exploited by WannaCry/WannaCrypt ransomware, EternalRocks worm and Petya ransomware.  **Vulnerability Fix**: Install patch for Windows 2008 R2.  **Severity: CRITICAL** |

|  |
| --- |
| Vulnerability in DNS Resolution Could Allow Remote Code Execution  **Synopsis:** MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution.  **Vulnerable Targets:**  [dc.ldil.de](http://dc.ldil.de) / 10.0.100.10  rodc.ldil.de / 192.168.10.10  **Vulnerability Explanation**: A remote code execution vulnerability exists in the way that the Windows DNS Server improperly handles a specially crafted NAPTR query string in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  **Vulnerability Fix**: Microsoft has released a set of patches for Windows 2003, 2008, and 2008 R2. [http://technet.microsoft.com/en-us/security/bulletin/ms11-058](http://technet.microsoft.com/en-us/security/bulletin/ms11-058" \t "_blank)  **Severity: HIGH** |

|  |
| --- |
| Vulnerability in Schannel Could Allow Remote Code Execution  **Synopsis:** The remote Windows host is affected by a remote code execution vulnerability.  **Vulnerable Targets:**  [dc.ldil.de](http://dc.ldil.de) / 10.0.100.10  **Vulnerability Explanation**:  Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)  An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)  **Vulnerability Fix**: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.  **Severity: HIGH** |

|  |
| --- |
| Vulnerability in DNS Resolution Could Allow Remote Code Execution  **Synopsis:** Arbitrary code can be executed on the remote host through the installed Windows DNS client.  **Vulnerable Targets:**  10.0.100.10 445/tcp Microsoft Windows SMB service  **Vulnerability Explanation**: The remote Windows host is affected by the following vulnerabilities:  Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)  An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)  **Vulnerability Fix**: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.  **Severity: HIGH** |

|  |
| --- |
| Outdated jQuery library in use  **Synopsis:** jQuery library is outdated and possibly vulnerable to exploits  **Vulnerable Targets:** <http://intra.ldil.de> / 10.0.100.30  **Vulnerability Explanation:** Ability Server 2.34 is subject to a buffer overflow vulnerability in STOR field. Attackers can use this vulnerability to cause arbitrary remote code execution and take completely control over the system.  Vulnerability Fix: Update jQuery as well as the dependent libraries to the latest version.  **Severity:** MEDIUM |

|  |
| --- |
| Outdated PHP version in use  **Synopsis:** PHP framework is outdated and possibly vulnerable to exploits  **Vulnerable Targets:** <http://intra.ldil.de> / 10.0.100.30  **Vulnerability Explanation**: Intra-server is running unsupported PHP framework version, meaning there is no longer fixes and updates received from the PHP community.  **Vulnerability Fix**: Update PHP to at least to the one of the supported versions. Current version is not supported and might contain vulnerabilities as the support is no longer extended.  Severity: MEDIUM |

|  |
| --- |
| Verbose information about system version available in http response  **Synopsis:** HTTP response includes information the operating system.  **Vulnerable Targets:** <http://intra.ldil.de> / 10.0.100.30  **Vulnerability Explanation**: HTTP response gives out unneeded information to the end user and thus compromising the system security.  **Vulnerability Fix**: Hide the verbose response of currently used software versions from the http response.  **Severity: MEDIUM** |

|  |
| --- |
| Verbose information about PHP and Apache version available in http response  **Synopsis:** Verbose information about the PHP and Apache versions present in http response.  **Vulnerable Targets:** <http://intra.ldil.de> / 10.0.100.30  **Vulnerability Explanation**: Exposing the system version information to end-users is not needed. If it is needed internally, use different methods than printing it to http responses in plain-text (“Hi! I am using version..”).  **Vulnerability Fix**: Disable unneeded information sharing to end-users.  **Severity: MEDIUM** |

|  |
| --- |
| Buffer overflow detected  **Synopsis:** Buffer overflow errors are happening when the overwriting of memory spaces of the background web process, which should never been modified intentionally or unintentionally. Overwriting values of the IP (instruction pointer), BP (base pointer) and other registers causes exceptions, segmentation faults and the other process errors to occur.  **Vulnerable Targets:** <http://intra.ldil.de> / 10.0.100.30  **Vulnerability Explanation**: Potential buffer overflow detected. The script closed the connection and threw a 500 Internal Server Error.  **Vulnerability Fix**: Rewrite the background program using proper return length checking. This will require a recompile of the background executable.  **Severity: MEDIUM**  **Proof of Concept Code Here:**  GET  <https://intra.ldil.de/wp-content/themes/twentysixteen?query=xlScCqlemqpPtXbFamPILdDaLkKPaUyLMWHUlAa>...... Basically any long enough query |

|  |
| --- |
| Directory browsing is enabled  **Synopsis:** Directory browsing is enabled and it is possible to view the directory listing  **Vulnerable Targets:** [https://intra.ldil.de/wp-admin /](https://intra.ldil.de/wp-admin%20/) 10.0.100.30  **Vulnerability Explanation**: It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files which can be accessed to read sensitive information.  **Vulnerability Fix**: Disable directory browsing. If the directory browsing cannot be disabled because of some other service needing it, make sure the listed files do not include any risks.  **Severity: MEDIUM** |

|  |
| --- |
| Format string error  **Synopsis**: A format string error occurs when the submitted data of an input string is evaluated as a command by the application.  **Vulnerable Targets:** <http://intra.ldil.de> / 10.0.100.30  **Vulnerability Explanation**: Potential format string error occurred. The script closed the connection on a /%s  **Vulnerability Fix**: Review the background program using proper deletion of bad character strings (parameterize). This will require a recompile of the background executable.  **Severity: MEDIUM** |

|  |
| --- |
| X-frame-options header not set  **Synopsis:** X-Frame-Options header is not included in the HTTP response  **Vulnerable Targets:**  <http://intra.ldil.de> / 10.0.100.30  <http://helpdesk.ldil.de> / 10.10.10.40  **Vulnerability Explanation**: X-Frame-Options header should be included in the HTTP response to protect against ClickJacking attacks.  **Vulnerability Fix**: Most modern web browsers support the X-Frame-Options HTTP header. Ensure it is set on all web pages returned to your site.  **Severity: MEDIUM** |

|  |
| --- |
| SSH Weak Algorithms Supported  **Synopsis:** The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.  **Vulnerable Targets:** pos.ldil.de / 192.168.10.20  **Vulnerability Explanation**: Remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.  **Vulnerability Fix**: Update and configure SSH server to disable weak algorithm.  **Severity: MEDIUM** |

|  |
| --- |
| HTTP TRACE / TRACK Methods Allowed  **Synopsis:** Debugging functions are enabled on the remote web server.  **Vulnerable Targets:** <http://pos.ldil.de> / 192.168.10.20  **Vulnerability Explanation**: The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.  **Vulnerability Fix**: Refer to Apache web server documentation on how to disable these methods.  **Severity: MEDIUM** |

|  |
| --- |
| XSS-protection is not enabled  **Synopsis:** Web browser XSS protection is not enabled or is disabled by the configuration of the X-XSS-Protection HTTP response header on the webserver.  **Vulnerable Targets:** <http://intra.ldil.de> / 10.0.100.30  **Vulnerability Explanation**: The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser´s XSS protection mechanisms. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block.  The X-XSS-Protection HTTP response header is currently supported on IE, Chrome and Safari.  **Vulnerability Fix**: Ensure that the web browser´s XSS filter is enabled by setting the X-XSS-Protection HTTP response header to “1”.  **Severity: MINOR** |

|  |
| --- |
|  |

# Sample Report – Attachments

Tiedostoina!!!

Nimeäminen:

* Segmentti\_Numero\_Työkalu\_Tarkenne

Sisältö:

* Nessus-raportit
* Openwas-raportit
* NMAP-raportit
* Zap-raportit
* OWASP-raportit

Esittäminen:

* Taulukko
  + Liitteen nimi
  + Sisältö

Table 9 Attachment files

|  |  |
| --- | --- |
| Attachment name | Attachment description |
| StoreBranch\_01\_Nessus\_portscan.pdf | Nessus port scan of store branch network segment |
| Internal\_02\_Nessus\_portscan.pdf | Nessus port scan of internal network segment |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |