Cybersecurity Status Report (NIS2)

Prepared by Red Code Company, LLC.

Report ID: [redacted]
Requested by: [redacted]

Company: [redacted]
Company website: [redacted]
Date: 2025-07-10 [redacted]
Report type: full
Checked hosts: 195
Subdomains found: 370
Hosts by Country: [redacted]

Summary

Critical CVEs: 13

Publicly known vulnerabilities with CVSS score 9.0–10.0, potentially linked to the evaluated entity.

Non-critical CVEs: 164

Public vulnerabilities with CVSS score below 9.0, identified via passive data analysis.

Total Leaks: 192

Number of records from breach archives or leak databases containing emails or domains related to the evaluated entity.

Ransomware Incident: No

OSINT indication (e.g., mentions on ransomware sites) of possible exposure — not a confirmation of compromise.

ORSI: 7

ORSI (Open Response Signal Index): An advanced analytical solution for automated digital exposure assessment based exclusively on publicly accessible data (OSINT). The score ranges from 0 (clean) to 10 (critical public footprint), reflecting the level of externally observable digital exposure

Data Source Statement:

All data in this report is sourced exclusively from publicly available information, including public vulnerability databases, cybersecurity bulletins, and technical metadata derived from open-source intelligence platforms.

NIS2 Directive Compliance:

This document supports internal cybersecurity evaluations in alignment with the following articles of the NIS2 Directive (EU 2022/2555):

- **Article 21 (Risk Management):** identification of publicly known vulnerabilities;
- **Article 23 (Vulnerability Handling & Monitoring):** use of passive CVE tracking and OSINT tools;
- **Article 24 (Incident Reporting):** recognition of ransomware mentions or indicators;
- **Article 26 (Supply Chain Security):** third-party surface analysis for dependency risks;
- **Article 30 (Notifications):** risk signals for internal reporting workflows;
- **Article 44 (Enforcement & Penalties):** contributes to traceability in risk posture oversight.

Legal Notice:

This report (ID: [redacted]) was prepared by Red Code Company, LLC at the request of [redacted] solely for internal evaluation purposes under Article 26 of the NIS2 Directive.

This report was prepared without the participation or prior consent of the evaluated entity, [redacted] *All observations are derived from open-source data and do not represent verified or authorized technical assessments.*

All findings are based entirely on passive observation of publicly accessible data. No active interaction, scanning, testing, or unauthorized access has occurred. No conclusion is made regarding actual compromise or system breach.

This document must not be interpreted as a security certification, vulnerability audit, or claim of factual security posture for the evaluated entity [redacted]

Redistribution, publication, or any third-party usage – including for enforcement, litigation, or media – is strictly prohibited without prior written authorization from Red Code Company, LLC.

Red Code Company, LLC
IČO: 22385151
Děčínská 552/1, Střížkov, 180 00 Prague 8
✉ info@redcode.company

Terms of Use for Cybersecurity Risk Reports

Issued by: Red Code Company, LLC IČO: 22385151 Děčínská 552/1, Střížkov, 180 00 Prague 8
Version: 1.0 **Effective Date:** 2025-06-02
*This Terms of Use section applies to the report titled "**Cybersecurity Status Report (NIS2)**", ID:* [redacted]

1. Purpose and Scope

This document outlines the conditions under which the cybersecurity risk assessment report (hereafter “the Report”) is provided by Red Code Company, LLC (“Provider”) to the requesting party (“Client”).

2. Use of Report

1. The Report is intended for internal evaluation purposes only.
2. The Report may not be distributed, published, or shared with third parties without prior written consent from Red Code Company, LLC.
3. The Report must not be used in media, legal proceedings, enforcement, or contractual negotiations.

3. Methodology

The Report is based solely on passive analysis of publicly accessible sources, including:

- Public CVE databases.
- Open-source intelligence platforms.
- DNS records, WHOIS, and breach repositories.

No active scanning, intrusion, penetration testing, or unauthorized access was conducted.

4. Explanation of Key Terms

- **Critical CVEs:** Publicly known vulnerabilities with CVSS score 9.0–10.0, potentially linked to the evaluated entity.
- **Non-critical CVEs:** Public vulnerabilities with CVSS score below 9.0, identified via passive data analysis.
- **Total Leaks:** Number of records from breach archives or leak databases containing emails or domains related to the evaluated entity.
- **Ransomware Incident:** OSINT indication (e.g., mentions on ransomware sites) of possible exposure — not a confirmation of compromise.
- **OSINT (Open-Source Intelligence):** Legally collected information from publicly available sources, excluding any interaction with the target systems.
- **ORSI (Open Response Signal Index):** An advanced analytical solution for automated digital exposure assessment based exclusively on publicly accessible data (OSINT). The score ranges from 0 (clean) to 10 (critical public footprint), reflecting the level of externally observable digital exposure.

5. Explanation of CVE Impact

- **Attack Vector (AV): N (Network):** Exploitable remotely over a network. **A (Adjacent):** Exploitable from adjacent network (e.g. same subnet). **L (Local):** Requires local access on the machine. **P (Physical):** Requires physical interaction (e.g. plugging in a device).
- **Attack Complexity (AC): L (Low):** “Low” complexity; no special conditions. **H (High):** “High” complexity; attacker needs specific conditions.
- **Privileges Required (PR): N (None):** No privileges needed. **L (Low):** Requires low-level privileges. **H (High):** Requires high-level privileges.
- **User Interaction (UI): N (None):** No user action required. **R (Required):** User must take some action.
- **Scope (S): U (Unchanged):** Exploitation does not affect other components. **C (Changed):** Exploitation can affect resources beyond the vulnerable component.
- **Confidentiality Impact (C): N (None):** No impact on confidentiality. **L (Low):** Partial information disclosure. **H (High):** Total information disclosure.
- **Integrity Impact (I): N (None):** No impact on integrity. **L (Low):** Some modification of data possible. **H (High):** Total compromise of integrity.
- **Availability Impact (A): N (None):** No impact on availability. **L (Low):** Performance degradation or partial outage. **H (High):** Total shutdown/denial of service.
- **Authentication (Au): N (None):** No authentication required. **S (Single):** Single instance of authentication required. **M (Multiple):** Multiple instances required.

6. No Guarantee or Warranty

- The Report does not certify, validate, or confirm the actual cybersecurity posture of the evaluated entity.
- The findings do not constitute a vulnerability assessment or security audit.
- Red Code Company, LLC makes no guarantee as to the accuracy, completeness, or impact of the data collected.

7. No Involvement of Evaluated Entity

The evaluated entity (subject of the Report) was not notified, did not participate, and did not authorize the creation of this Report.

8. Liability and Acceptance

Red Code Company, LLC shall not be held liable for any use, misuse, or interpretation of the Report. The Client assumes full responsibility for risk interpretation and further action.

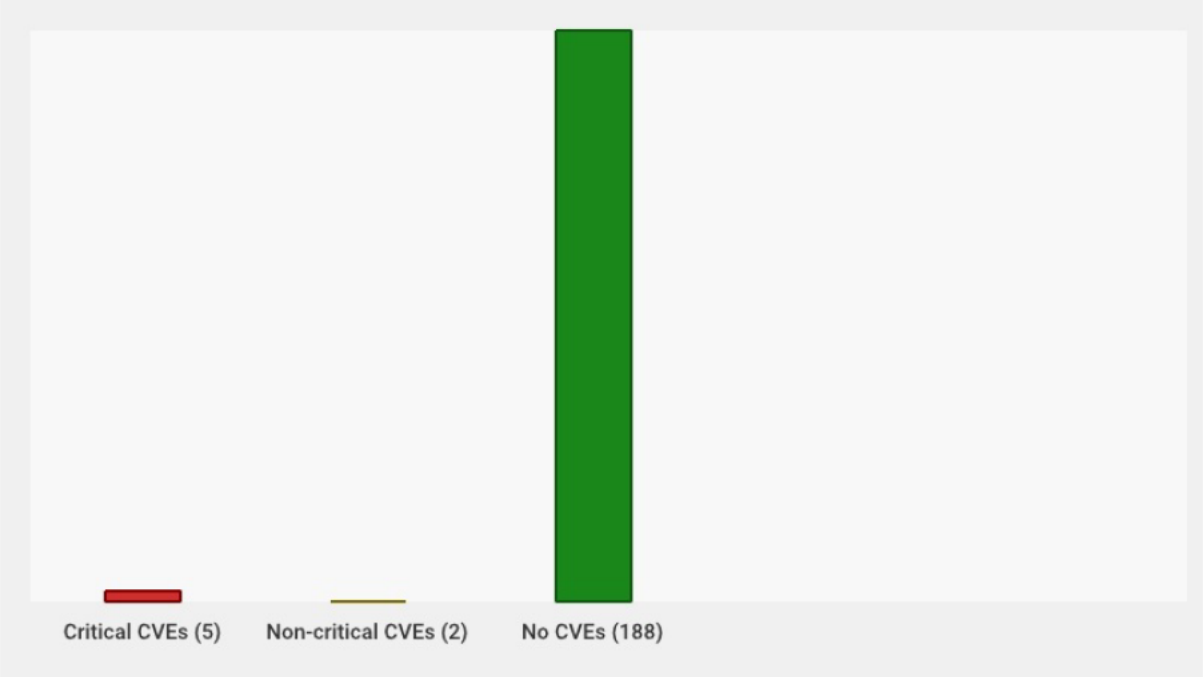
Use of the Report constitutes acceptance of these Terms of Use. If you do not agree, you must refrain from accessing, copying, or referencing the Report.

Report ID: [redacted]

Infrastructure Exposure Breakdown by Severity and Location

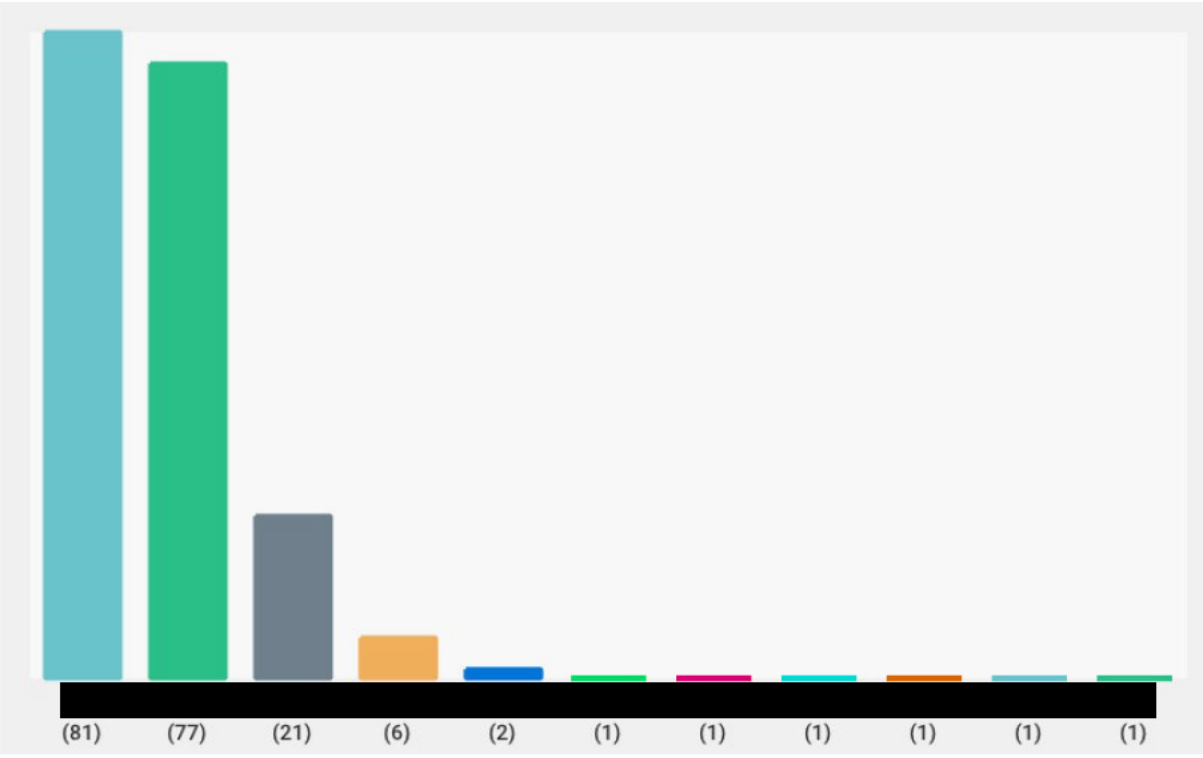
Host Security Overview

This chart summarizes the distribution of checked hosts by the severity of detected CVEs (Critical, Non-critical, or None). It provides a quick overview of the external vulnerability landscape for your infrastructure.



Hosts by Country

This chart shows the geographic distribution of all discovered hosts. Geographic spread helps assess regional exposure and identify possible compliance or risk hot spots.



Checked hosts: 195 **Subdomains found:** 370

Report ID: [redacted]

Discovered Vulnerable Services and Ports by Host

Host: [redacted]

Port	Transport	Product	Version	CVEs
22	tcp	[redacted]	[redacted]	CVE-2025-26465, CVE-2023-51767, CVE-2007-2768, CVE-2025-32728, CVE-2008-3844, CVE-2025-26466

Host: [redacted]

Port	Transport	Product	Version	CVEs
80	tcp	[redacted]	[redacted]	CVE-2019-9511, CVE-2018-16843, CVE-2021-3618, CVE-2018-16844, CVE-2019-9516, CVE-2019-9513, CVE-2021-23017, CVE-2019-20372, CVE-2018-16845, CVE-2023-44487

Host: [redacted]

Port	Transport	Product	Version	CVEs
80	tcp	[redacted]	[redacted]	CVE-2023-44487, CVE-2021-23017, CVE-2021-3618
443	tcp	[redacted]	[redacted]	CVE-2023-44487, CVE-2021-23017, CVE-2021-3618

Host: [redacted]

Port	Transport	Product	Version	CVEs
443	tcp	[redacted]	[redacted]	CVE-2013-2765, CVE-2021-32792, CVE-2023-31122, CVE-2021-34798, CVE-2013-0942, CVE-2021-26691, CVE-2024-40898, CVE-2022-28615, CVE-2019-0190, CVE-2019-0211, CVE-2019-10092, CVE-2012-4001, CVE-2021-40438, CVE-2020-35452, CVE-2020-13938, CVE-2022-30556, CVE-2022-22719, CVE-2021-36160, CVE-2021-32786, CVE-2020-11984, CVE-2019-0217, CVE-2020-1927, CVE-2024-27316, CVE-2024-38476, CVE-2019-10098, CVE-2019-0220, CVE-2022-36760, CVE-2022-29404, CVE-2022-22721, CVE-2011-1176, CVE-2022-28614, CVE-2021-32791, CVE-2021-33193, CVE-2022-31813, CVE-2022-37436, CVE-2011-2688, CVE-2022-26377, CVE-2022-28330, CVE-2019-9517, CVE-2024-38475, CVE-2012-4360, CVE-2019-0215, CVE-2022-23943, CVE-2023-25690, CVE-2007-4723, CVE-2020-11993, CVE-2013-0941, CVE-2020-1934, CVE-2024-38474, CVE-2018-17199, CVE-2021-44790, CVE-2021-39275, CVE-2019-0196, CVE-2009-0796, CVE-2024-38477, CVE-2019-17567, CVE-2019-10097, CVE-2021-32785, CVE-2021-44224, CVE-2019-10081, CVE-2023-27522, CVE-2022-22720, CVE-2023-45802, CVE-2019-10082, CVE-2020-9490, CVE-2021-26690, CVE-2018-17189, CVE-2013-4365, CVE-2006-20001, CVE-2019-0197, CVE-2012-3526, CVE-2009-2299

Host: [redacted]

Port	Transport	Product	Version	CVEs
22	tcp	[redacted]	[redacted]	CVE-2007-2768, CVE-2025-32728, CVE-2008-3844, CVE-2025-26466, CVE-2025-26465, CVE-2023-51767

Host: [redacted]

Port	Transport	Product	Version	CVEs
80	tcp	[redacted]	[redacted]	CVE-2020-1934, CVE-2018-17189, CVE-2022-29404, CVE-2024-38476, CVE-2021-40438, CVE-2011-2688, CVE-2013-2765, CVE-2013-4365, CVE-2019-0211, CVE-2011-1176, CVE-2021-32786, CVE-2022-28615, CVE-2023-31122, CVE-2021-44790, CVE-2021-32791, CVE-2022-22721, CVE-2022-31813, CVE-2012-4360, CVE-2022-23943, CVE-2022-28614, CVE-2018-1312, CVE-2012-3526, CVE-2013-0941, CVE-2022-37436, CVE-2018-17199, CVE-2019-0220, CVE-2021-34798, CVE-2022-22719, CVE-2018-11763, CVE-2017-15710, CVE-2019-0196, CVE-2022-36760, CVE-2021-33193, CVE-2021-32792, CVE-2018-1302, CVE-2019-10082, CVE-2009-2299, CVE-2022-22720, CVE-2022-28330, CVE-2013-0942, CVE-2021-26690, CVE-2018-1283, CVE-2018-1333, CVE-2019-9517, CVE-2019-10098, CVE-2023-25690, CVE-2020-9490, CVE-2024-38474, CVE-2012-4001, CVE-2024-40898, CVE-2018-1303, CVE-2023-45802, CVE-2020-13938, CVE-2022-30556, CVE-2021-44224, CVE-2024-38475, CVE-2006-20001, CVE-2024-27316, CVE-2020-35452, CVE-2009-0796, CVE-2024-38477, CVE-2019-17567, CVE-2017-15715, CVE-2

				018-1301, CVE-2019-10092, CVE-2021-32785, CVE-2021-26691, CVE-2022-26377, CVE-2019-0217, CVE-2021-39275, CVE-2020-11993, CVE-2020-1927, CVE-2007-4723, CVE-2019-10081
443	tcp	[redacted]	[redacted]	CVE-2021-32791, CVE-2022-23943, CVE-2020-1927, CVE-2021-33193, CVE-2022-22720, CVE-2020-11993, CVE-2021-26691, CVE-2009-0796, CVE-2018-1333, CVE-2023-25690, CVE-2022-28330, CVE-2019-17567, CVE-2022-37436, CVE-2011-2688, CVE-2006-20001, CVE-2018-17199, CVE-2020-9490, CVE-2023-45802, CVE-2019-10082, CVE-2012-3526, CVE-2024-38477, CVE-2024-38475, CVE-2024-27316, CVE-2020-1934, CVE-2022-28614, CVE-2020-13938, CVE-2024-40898, CVE-2022-29404, CVE-2019-9517, CVE-2021-40438, CVE-2019-0220, CVE-2021-39275, CVE-2013-2765, CVE-2024-38476, CVE-2022-26377, CVE-2019-0217, CVE-2022-31813, CVE-2012-4360, CVE-2022-36760, CVE-2013-0941, CVE-2011-1176, CVE-2017-15710, CVE-2021-44790, CVE-2018-1312, CVE-2019-0196, CVE-2017-15715, CVE-2021-32785, CVE-2022-30556, CVE-2018-11763, CVE-2019-0211, CVE-2022-22721, CVE-2013-0942, CVE-2023-31122, CVE-2024-38474, CVE-2021-34798, CVE-2021-44224, CVE-2019-10081, CVE-2018-1283, CVE-2018-1301, CVE-2018-1303, CVE-2021-32786, CVE-2007-4723, CVE-2020-35452, CVE-2013-4365, CVE-2019-10092, CVE-2019-10098, CVE-2018-17189, CVE-2021-32792, CVE-2012-4001, CVE-2022-28615, CVE-2018-1302, CVE-2021-26690, CVE-2009-2299, CVE-2022-22719

Host: [redacted]

Port	Transport	Product	Version	CVEs
22	tcp	[redacted]	[redacted]	CVE-2008-3844, CVE-2025-26466, CVE-2025-26465, CVE-2023-51767, CVE-2007-2768, CVE-2025-32728

CVEs overview

Critical CVEs (CVSS 8–10)

1. CVE-2008-3844 | CVSS: 9.3 | Impact: (AV:N/AC:M/Au:N/C:C/I:C/A:C) | Host: [redacted] | Country: [redacted]
2. CVE-2008-3844 | CVSS: 9.3 | Impact: (AV:N/AC:M/Au:N/C:C/I:C/A:C) | Host: [redacted] | Country: [redacted]
3. CVE-2024-38474 | CVSS: 9.8 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]
4. CVE-2024-38475 | CVSS: 9.1 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N) | Host: [redacted] | Country: [redacted]
5. CVE-2023-25690 | CVSS: 9.8 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]
6. CVE-2022-36760 | CVSS: 9 | Impact: (AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]
7. CVE-2024-38476 | CVSS: 9.8 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]
8. CVE-2008-3844 | CVSS: 9.3 | Impact: (AV:N/AC:M/Au:N/C:C/I:C/A:C) | Host: [redacted] | Country: [redacted]
9. CVE-2024-38476 | CVSS: 9.8 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]
10. CVE-2024-38474 | CVSS: 9.8 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]
11. CVE-2022-36760 | CVSS: 9 | Impact: (AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]
12. CVE-2024-38475 | CVSS: 9.1 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N) | Host: [redacted] | Country: [redacted]
13. CVE-2023-25690 | CVSS: 9.8 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]

Non-critical CVEs (CVSS 0–7.9)

1. CVE-2025-26466 | CVSS: 5.9 | Impact: (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
2. CVE-2025-26465 | CVSS: 6.8 | Impact: (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N) | Host: [redacted] | Country: [redacted]
3. CVE-2023-51767 | CVSS: 7 | Impact: (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]
4. CVE-2007-2768 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
5. CVE-2025-32728 | CVSS: 4.3 | Impact: (AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N) | Host: [redacted] | Country: [redacted]
6. CVE-2007-2768 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
7. CVE-2025-32728 | CVSS: 4.3 | Impact: (AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N) | Host: [redacted] | Country: [redacted]

8. CVE-2025-26466 | CVSS: 5.9 | Impact: (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
9. CVE-2025-26465 | CVSS: 6.8 | Impact: (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N) | Host: [redacted] | Country: [redacted]
10. CVE-2023-51767 | CVSS: 7 | Impact: (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]
11. CVE-2019-20372 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
12. CVE-2018-16844 | CVSS: 7.8 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:C) | Host: [redacted] | Country: [redacted]
13. CVE-2019-9516 | CVSS: 6.8 | Impact: (AV:N/AC:L/Au:S/C:N/I:N/A:C) | Host: [redacted] | Country: [redacted]
14. CVE-2019-9513 | CVSS: 7.8 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:C) | Host: [redacted] | Country: [redacted]
15. CVE-2021-23017 | CVSS: 6.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
16. CVE-2021-3618 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:N) | Host: [redacted] | Country: [redacted]
17. CVE-2018-16845 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:N/A:P) | Host: [redacted] | Country: [redacted]
18. CVE-2023-44487 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
19. CVE-2019-9511 | CVSS: 7.8 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:C) | Host: [redacted] | Country: [redacted]
20. CVE-2018-16843 | CVSS: 7.8 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:C) | Host: [redacted] | Country: [redacted]
21. CVE-2023-44487 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
22. CVE-2021-23017 | CVSS: 6.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
23. CVE-2021-3618 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:N) | Host: [redacted] | Country: [redacted]
24. CVE-2021-32785 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
25. CVE-2019-9517 | CVSS: 7.8 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:C) | Host: [redacted] | Country: [redacted]
26. CVE-2022-22721 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:P) | Host: [redacted] | Country: [redacted]
27. CVE-2022-28330 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
28. CVE-2021-36160 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
29. CVE-2019-0197 | CVSS: 4.9 | Impact: (AV:N/AC:M/Au:S/C:N/I:P/A:P) | Host: [redacted] | Country: [redacted]
30. CVE-2024-38477 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
31. CVE-2022-28615 | CVSS: 6.4 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:P) | Host: [redacted] | Country: [redacted]
32. CVE-2021-44790 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
33. CVE-2019-10082 | CVSS: 6.4 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:P) | Host: [redacted] | Country: [redacted]
34. CVE-2022-30556 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
35. CVE-2011-1176 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
36. CVE-2020-9490 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
37. CVE-2021-44224 | CVSS: 6.4 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:P) | Host: [redacted] | Country: [redacted]
38. CVE-2012-3526 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
39. CVE-2019-10097 | CVSS: 6 | Impact: (AV:N/AC:M/Au:S/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
40. CVE-2022-22720 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
41. CVE-2022-26377 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
42. CVE-2013-0941 | CVSS: 2.1 | Impact: (AV:L/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
43. CVE-2007-4723 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
44. CVE-2019-10092 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
45. CVE-2019-0211 | CVSS: 7.2 | Impact: (AV:L/AC:L/Au:N/C:C/I:C/A:C) | Host: [redacted] | Country: [redacted]
46. CVE-2009-0796 | CVSS: 2.6 | Impact: (AV:N/AC:H/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
47. CVE-2013-4365 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
48. CVE-2022-22719 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
49. CVE-2023-31122 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
50. CVE-2018-17189 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
51. CVE-2020-11993 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
52. CVE-2024-27316 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]

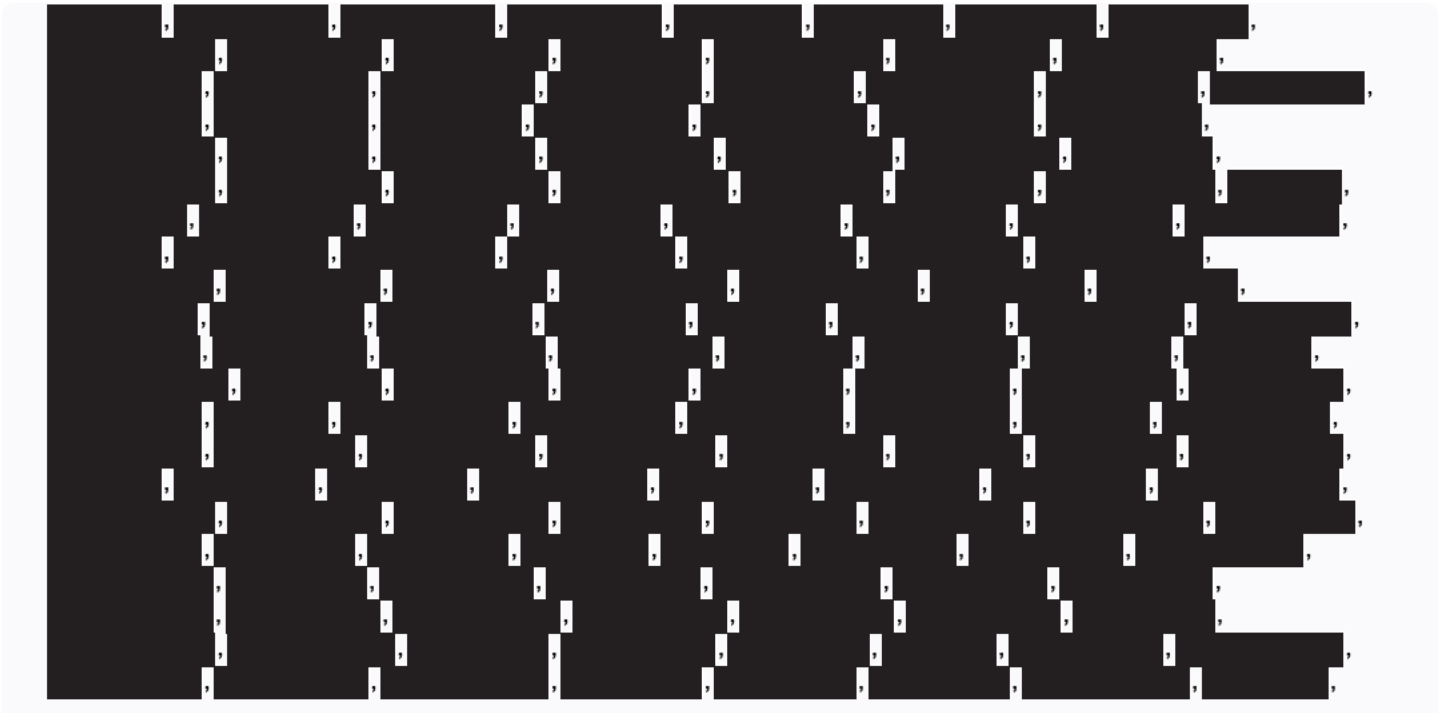
53. CVE-2019-10081 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
54. CVE-2013-0942 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
55. CVE-2011-2688 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
56. CVE-2023-45802 | CVSS: 5.9 | Impact: (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
57. CVE-2022-29404 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
58. CVE-2021-40438 | CVSS: 6.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
59. CVE-2022-23943 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
60. CVE-2020-35452 | CVSS: 6.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
61. CVE-2019-0196 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
62. CVE-2021-32792 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
63. CVE-2019-0215 | CVSS: 6 | Impact: (AV:N/AC:M/Au:S/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
64. CVE-2012-4001 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
65. CVE-2009-2299 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
66. CVE-2021-34798 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
67. CVE-2022-28614 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
68. CVE-2020-1934 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
69. CVE-2020-1927 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:N) | Host: [redacted] | Country: [redacted]
70. CVE-2018-17199 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
71. CVE-2021-32786 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:N) | Host: [redacted] | Country: [redacted]
72. CVE-2024-40898 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) | Host: [redacted] | Country: [redacted]
73. CVE-2021-26691 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
74. CVE-2019-0220 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
75. CVE-2021-33193 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
76. CVE-2006-20001 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
77. CVE-2022-31813 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
78. CVE-2020-11984 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
79. CVE-2020-13938 | CVSS: 2.1 | Impact: (AV:L/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
80. CVE-2021-32791 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
81. CVE-2019-0190 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
82. CVE-2013-2765 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
83. CVE-2023-27522 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N) | Host: [redacted] | Country: [redacted]
84. CVE-2022-37436 | CVSS: 5.3 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N) | Host: [redacted] | Country: [redacted]
85. CVE-2012-4360 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
86. CVE-2021-26690 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
87. CVE-2019-17567 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
88. CVE-2019-0217 | CVSS: 6 | Impact: (AV:N/AC:M/Au:S/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
89. CVE-2019-10098 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:N) | Host: [redacted] | Country: [redacted]
90. CVE-2021-39275 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
91. CVE-2007-2768 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
92. CVE-2025-32728 | CVSS: 4.3 | Impact: (AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N) | Host: [redacted] | Country: [redacted]
93. CVE-2025-26466 | CVSS: 5.9 | Impact: (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
94. CVE-2025-26465 | CVSS: 6.8 | Impact: (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N) | Host: [redacted] | Country: [redacted]
95. CVE-2023-51767 | CVSS: 7 | Impact: (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) | Host: [redacted] | Country: [redacted]
96. CVE-2020-35452 | CVSS: 6.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]

97. CVE-2012-4360 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
98. CVE-2013-0942 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
99. CVE-2006-20001 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
100. CVE-2021-44224 | CVSS: 6.4 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:P) | Host: [redacted] | Country: [redacted]
101. CVE-2022-30556 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
102. CVE-2021-39275 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
103. CVE-2020-11993 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
104. CVE-2019-0196 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
105. CVE-2009-0796 | CVSS: 2.6 | Impact: (AV:N/AC:H/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
106. CVE-2011-2688 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
107. CVE-2019-10098 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:N) | Host: [redacted] | Country: [redacted]
108. CVE-2021-26690 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
109. CVE-2020-9490 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
110. CVE-2022-31813 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
111. CVE-2022-28615 | CVSS: 6.4 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:P) | Host: [redacted] | Country: [redacted]
112. CVE-2019-17567 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
113. CVE-2020-1934 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
114. CVE-2024-27316 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
115. CVE-2019-0220 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
116. CVE-2019-10082 | CVSS: 6.4 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:P) | Host: [redacted] | Country: [redacted]
117. CVE-2012-3526 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
118. CVE-2022-22721 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:P) | Host: [redacted] | Country: [redacted]
119. CVE-2021-33193 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
120. CVE-2022-37436 | CVSS: 5.3 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N) | Host: [redacted] | Country: [redacted]
121. CVE-2021-26691 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
122. CVE-2024-38477 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
123. CVE-2021-40438 | CVSS: 6.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
124. CVE-2011-1176 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
125. CVE-2018-1302 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
126. CVE-2021-32785 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
127. CVE-2007-4723 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
128. CVE-2013-4365 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
129. CVE-2019-0211 | CVSS: 7.2 | Impact: (AV:L/AC:L/Au:N/C:C/I:C/A:C) | Host: [redacted] | Country: [redacted]
130. CVE-2022-23943 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
131. CVE-2019-10081 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
132. CVE-2009-2299 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
133. CVE-2021-44790 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
134. CVE-2020-1927 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:N) | Host: [redacted] | Country: [redacted]
135. CVE-2022-22720 | CVSS: 7.5 | Impact: (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
136. CVE-2017-15715 | CVSS: 6.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
137. CVE-2018-17189 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
138. CVE-2022-29404 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
139. CVE-2018-11763 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
140. CVE-2022-22719 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]

141. CVE-2018-17199 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
142. CVE-2017-15710 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
143. CVE-2021-34798 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
144. CVE-2022-28614 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
145. CVE-2020-13938 | CVSS: 2.1 | Impact: (AV:L/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
146. CVE-2018-1333 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
147. CVE-2021-32792 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
148. CVE-2012-4001 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
149. CVE-2019-0217 | CVSS: 6 | Impact: (AV:N/AC:M/Au:S/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]
150. CVE-2018-1301 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
151. CVE-2013-0941 | CVSS: 2.1 | Impact: (AV:L/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
152. CVE-2021-32786 | CVSS: 5.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:N) | Host: [redacted] | Country: [redacted]
153. CVE-2019-9517 | CVSS: 7.8 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:C) | Host: [redacted] | Country: [redacted]
154. CVE-2018-1283 | CVSS: 3.5 | Impact: (AV:N/AC:M/Au:S/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
155. CVE-2022-28330 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
156. CVE-2021-32791 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:P/I:N/A:N) | Host: [redacted] | Country: [redacted]
157. CVE-2022-26377 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
158. CVE-2018-1303 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
159. CVE-2019-10092 | CVSS: 4.3 | Impact: (AV:N/AC:M/Au:N/C:N/I:P/A:N) | Host: [redacted] | Country: [redacted]
160. CVE 2023 45802 | CVSS: 5.9 | Impact: (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
161. CVE-2023-31122 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | Host: [redacted] | Country: [redacted]
162. CVE-2024-40898 | CVSS: 7.5 | Impact: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) | Host: [redacted] | Country: [redacted]
163. CVE-2013-2765 | CVSS: 5 | Impact: (AV:N/AC:L/Au:N/C:N/I:N/A:P) | Host: [redacted] | Country: [redacted]
164. CVE-2018-1312 | CVSS: 6.8 | Impact: (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Host: [redacted] | Country: [redacted]

Hosts found

All identified hosts are public entry points to the company's digital infrastructure and require regular security monitoring.



[redacted]

Subdomains found

All identified subdomains are public entry points to the company’s digital infrastructure and require regular security monitoring.