XSPECTRE

SAMPLE REPORT — FICTIONAL DATA

Vulnerability Assessment Report

Example Pty Ltd · example.com

Report type	Technical Assessment
Report level	Advanced (Professional plan)
Scan date	14 November 2026
Issued	15 November 2026
Reference	XS-SAMPLE-2026-11

This is a sample. Example Pty Ltd, its people, hosts and findings are fictional, and the IP addresses are documentation and private ranges. Sample report — fictional data — xSPECTRE.

1 · EXECUTIVE SUMMARY

Your security at a glance

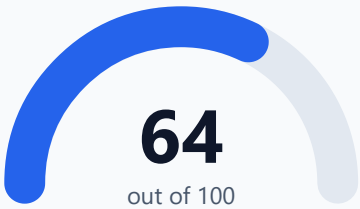
54 issues are open, down from 61 last month. One needs action now: the public web server runs a version that no longer gets security updates. Four High findings, including Remote Desktop open to the internet, should be fixed within the week.

SECURITY POSTURE GRADE

C

Last month: D

HEALTH SCORE

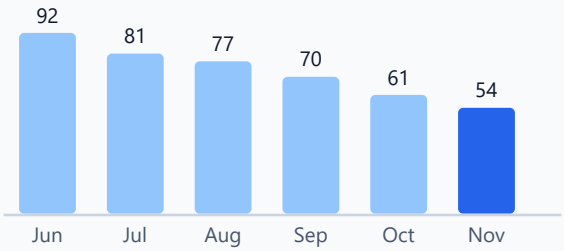


64

out of 100

Last month: 58

OPEN FINDINGS OVER THE LAST SIX SCHEDULED SCANS



Down 38 since June. Historical trending is included on Professional and Enterprise.

CRITICAL	HIGH	MEDIUM	LOW
1	4	12	37

Top risks in plain English

1. **The main website runs software that is no longer supported (XS-01).** New flaws in it will never be fixed. Upgrade it this week.
2. **Anyone on the internet can try to log in to a company server (XS-02).** Remote Desktop is open to the world. Put it behind a VPN with multi-factor authentication.
3. **The VPN gateway has a known flaw that can allow a takeover (XS-03).** One upgrade fixes this and a related weakness (XS-06).
4. **An old file server inside the office is open to WannaCry-style malware (XS-04).** Patch it or switch it off.

What has improved: since last month's scan, 11 findings are no longer detected and 4 new ones appeared. Cleared items include an expired certificate on the portal and two outdated printer firmware versions. Scheduled rescans show what is still detected, so progress is visible in each report.

2 · SCOPE AND METHOD

What we checked and how

This report covers the scheduled scan of 14 Nov 2026, 01:00–04:35 AEDT. Scans are automated and non-destructive: they look for known weaknesses and risky settings without trying to break in.

SCAN	HOW IT WORKS	IN SCOPE
Network Scans — perimeter	Scanned from the internet against your public IP addresses, the same view an attacker has.	7 public IP addresses in 203.0.113.0/24 (www, mail, portal, VPN gateway, remote access and two spare addresses)
Network Scans — internal	Run from the xSPECTRE scanner appliance installed on your network, so internal servers, PCs, printers and network devices are covered without opening firewall ports.	38 live assets across 10.20.1.0/24 (servers), 10.20.2.0/24 (file and print) and 10.20.3.0/24 (network devices)
Web Scans	Automated checks of your websites and web applications for common weaknesses such as insecure configuration, missing protections and outdated components.	2 web applications: https://www.example.com and https://portal.example.com

How findings are rated

Each finding has a CVSS v3.1 base score from 0 to 10. Where a public CVE exists we use the score published by the National Vulnerability Database (NVD). Configuration issues without a CVE carry an xSPECTRE-assessed score, shown with its vector.

Critical	9.0–10.0	Act now
High	7.0–8.9	Fix within days
Medium	4.0–6.9	Plan a fix
Low	0.1–3.9	Fix when convenient

Limits of this report

- It shows what was detected at the time of the scan. New issues can appear between scans.
- Automated scanning finds known weaknesses; it cannot find every issue, and a small number of results may be false positives.
- Web Scans in this sample were unauthenticated, so pages behind a login were not tested.
- Penetration testing (a person actively trying to break in) is a separate service.
- Scheduled rescans show what is still detected after you make changes.

3 · FINDINGS SUMMARY

Findings that need attention

The 8 findings below are explained in detail in section 4. The remaining 9 Medium and 37 Low findings are listed in the vulnerability register in your xSPECTRE portal, each with its own solution.

ID	FINDING	SEVERITY	CVSS	AFFECTED ASSETS
XS-01	**Web server version no longer supported**	Critical	9.8	www.example.com (203.0.113.30) — 443/tcp, 80/tcp
XS-02	**Remote Desktop (RDP) open to the internet**	High	8.1	203.0.113.24 — 3389/tcp (Microsoft Remote Desktop)
XS-03	**OpenSSH remote code execution (regreSSHion)** CVE-2024-6387	High	8.1	vpn.example.com (203.0.113.10) — 22/tcp
XS-04	**Windows SMBv1 remote code execution (MS17-010)** CVE-2017-0144	High	8.8	FS-OLD01 (10.20.2.30) — 445/tcp
XS-05	**Old TLS versions (1.0 and 1.1) still enabled**	High	7.4	mail.example.com (203.0.113.31) — 443/tcp, 587/tcp
XS-06	**SSH prefix truncation weakness (Terrapin)** CVE-2023-48795	Medium	5.9	vpn.example.com (203.0.113.10) — 22/tcp
XS-07	**Security headers missing on the customer portal**	Medium	5.4	https://portal.example.com
XS-08	**SNMP default community string ("public")**	Medium	6.5	SW-CORE02 (10.20.3.40) — 161/udp
–	**Other findings** Outdated software, weak settings and information leaks	Medium Low	0.1–6.9	9 Medium, 37 Low across 21 assets

4 · DETAILED FINDINGS

What we found, why it matters and how to fix it

Evidence is shortened and sanitised. Each finding is also listed in the vulnerability register in your xSPECTRE portal.

XS-01

Web server version no longer supported

Critical

9.8

CVSS v3.1

SUMMARY

Your public website runs nginx 1.18.0. This version stopped receiving security fixes in 2021, so weaknesses found since then will never be patched on it.

AFFECTED

www.example.com (203.0.113.30) — 443/tcp, 80/tcp

Found by Network Scans (perimeter), Web Scans

EVIDENCE

```
GET / HTTP/1.1  Host: www.example.com
HTTP/1.1 200 OK
Server: nginx/1.18.0
Detected version 1.18.0 — outside the vendor's supported branches
```

IMPACT

An attacker can look up public weaknesses for this exact version. Depending on how the server is configured, that could let them crash the website or, in the worst case, run their own code on the server that hosts it.

SOLUTION

1. Upgrade nginx to the current stable or mainline release from the vendor or your operating system's supported packages.
2. If the server is managed by a hosting provider or IT provider, ask them to upgrade it and confirm the new version in writing.
3. Hide the exact version in the Server header (server_tokens off) once upgraded.

SCORE

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`

xSPECTRE assessment for unsupported software (no single CVE).

REFERENCES

- nginx security advisories — nginx.org/en/security_advisories.html
- Example of a known issue fixed in later versions: CVE-2021-23017 (CVSS 3.1 7.7, NVD)

XS-02

Remote Desktop (RDP) open to the internet

High

8.1

CVSS v3.1

SUMMARY

A Windows server accepts Remote Desktop connections directly from the internet. Exposed Remote Desktop is one of the most common ways attackers break into businesses.

AFFECTED

203.0.113.24 — 3389/tcp (Microsoft Remote Desktop)
Found by Network Scans (perimeter)

EVIDENCE

```
3389/tcp open  ms-wbt-server
TLS certificate subject: CN=EX-RDS01.corp.example.com
Network Level Authentication: required
```

IMPACT

Anyone on the internet can try passwords against this server. A guessed, reused or leaked password would give an attacker a desktop inside your network, which is a common first step in ransomware attacks.

SOLUTION

1. Block 3389/tcp at the firewall for internet traffic.
2. Provide remote access through a VPN or remote desktop gateway that requires multi-factor authentication.
3. Review the server's sign-in logs for failed and unusual logins.

SCORE

`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H`
xSPECTRE assessment for an exposed remote-administration service (no single CVE).

REFERENCES

- ACSC — Essential Eight: multi-factor authentication and restrict administrative privileges (cyber.gov.au)
- Microsoft — Secure Remote Desktop with Remote Desktop Gateway

XS-03 · CVE-2024-6387

OpenSSH remote code execution (regreSSHion)

High

8.1

CVSS v3.1

SUMMARY

The SSH service on your VPN gateway runs OpenSSH 9.3p1, which is affected by a known flaw that can let an attacker run code on the server without logging in.

AFFECTED

vpn.example.com (203.0.113.10) — 22/tcp
Found by Network Scans (perimeter)

EVIDENCE

```
22/tcp open  ssh
Banner: SSH-2.0-OpenSSH_9.3p1
Affected range: 8.5p1 up to (not including) 9.8p1
```

IMPACT

Successful exploitation gives an attacker full control of the gateway. The attack is difficult and slow to carry out, which is why the score is High rather than Critical, but public research on it exists.

SOLUTION

1. Upgrade OpenSSH to 9.8p1 or later, or apply your operating system vendor's patched package.
2. Limit SSH on 22/tcp to known management addresses instead of the whole internet.
3. The same upgrade also fixes XS-06.

SCORE

`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H`

Base score as published by NVD.

REFERENCES

- NVD — CVE-2024-6387 (nvd.nist.gov)
- OpenSSH 9.8 release notes — openssh.com/releasenotes.html

XS-04 · CVE-2017-0144

Windows SMBv1 remote code execution (MS17-010)

High

8.8

CVSS v3.1

SUMMARY

An older internal file server still has SMB version 1 enabled and is missing the MS17-010 security update. This is the weakness used by the WannaCry and NotPetya outbreaks.

AFFECTED

FS-OLD01 (10.20.2.30) — 445/tcp

Found by Network Scans (internal, via scanner appliance)

EVIDENCE

```
445/tcp open  microsoft-ds
SMBv1 dialect accepted (NT LM 0.12)
MS17-010 security update not detected
```

IMPACT

Malware or an attacker already inside your network could use this to take over the server and spread to other computers. File servers often hold sensitive business data.

SOLUTION

1. Apply the Microsoft MS17-010 security update, or decommission the server if it is no longer needed.
2. Disable SMBv1 on this server and across the network.
3. Check other internal servers in the vulnerability register for the same issue.

SCORE

`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`

Base score as published by NVD.

REFERENCES

- Microsoft Security Bulletin MS17-010
- NVD — CVE-2017-0144 (nvd.nist.gov)

XS-05

Old TLS versions (1.0 and 1.1) still enabled

High

7.4

CVSS v3.1

SUMMARY

The mail server still accepts TLS 1.0 and TLS 1.1. Both versions are formally deprecated and have known weaknesses.

AFFECTED

mail.example.com (203.0.113.31) — 443/tcp, 587/tcp

Found by Network Scans (perimeter)

EVIDENCE

```
Accepted protocols: TLSv1.0, TLSv1.1, TLSv1.2
TLSv1.3: not offered
```

IMPACT

An attacker who can intercept traffic (for example on public Wi-Fi) has a better chance of reading or altering webmail sessions and mail in transit. Some insurers and auditors also flag old TLS as a control gap.

SOLUTION

1. Disable TLS 1.0 and 1.1 in the mail server and webmail configuration.
2. Allow TLS 1.2 and TLS 1.3 only, with modern cipher suites.

SCORE

`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N`

xSPECTRE assessment for deprecated protocol support (no single CVE).

REFERENCES

- RFC 8996 — Deprecating TLS 1.0 and TLS 1.1
- ACSC — Guidelines for Cryptography (ISM)

XS-06 · CVE-2023-48795

SSH prefix truncation weakness (Terrapin)

Medium

5.9

CVSS v3.1

SUMMARY

The SSH service offers encryption modes affected by the Terrapin weakness and does not support the "strict key exchange" protection.

AFFECTED

vpn.example.com (203.0.113.10) — 22/tcp

Found by Network Scans (perimeter)

EVIDENCE

```
Offered: chacha20-poly1305@openssh.com
Strict key exchange (kex-strict-s-v00@openssh.com): not supported
```

IMPACT

An attacker in a position to intercept the connection could weaken some security protections of the SSH session. It does not on its own expose passwords or data.

SOLUTION

1. Upgrade OpenSSH (fixed from 9.6). The upgrade for XS-03 resolves this as well.

SCORE

`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N`

Base score as published by NVD.

REFERENCES

- NVD — CVE-2023-48795 (nvd.nist.gov)
- terrapin-attack.com

XS-07

Security headers missing on the customer portal

Medium

5.4

CVSS v3.1

SUMMARY

The customer portal does not send several standard security headers that tell browsers how to protect your users.

AFFECTED

https://portal.example.com

Found by Web Scans

EVIDENCE

```
GET /login HTTP/1.1  Host: portal.example.com
Missing: Content-Security-Policy
Missing: Strict-Transport-Security
Missing: X-Content-Type-Options
```

IMPACT

Without these headers, attacks such as cross-site scripting and clickjacking are easier to carry out against people using the portal, and browsers may connect over unencrypted HTTP.

SOLUTION

1. Add Strict-Transport-Security, X-Content-Type-Options: nosniff and a Content-Security-Policy suited to the portal.
2. Add a frame-ancestors rule (or X-Frame-Options) to stop the portal being framed by other sites.

SCORE

`CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N`

xSPECTRE assessment for missing browser protections (no single CVE).

REFERENCES

- OWASP Secure Headers Project (owasp.org)
- MDN Web Docs — HTTP headers

XS-08

SNMP default community string ("public")

Medium

6.5

CVSS v3.1

SUMMARY

A core network switch answers SNMP requests using the default community string "public", which works like a well-known password.

AFFECTED

SW-CORE02 (10.20.3.40) — 161/udp

Found by Network Scans (internal, via scanner appliance)

EVIDENCE

```
161/udp open  snmp
SNMPv2c community "public" accepted (read-only)
sysDescr returned device model and firmware
```

IMPACT

Anyone on the internal network can read the switch's configuration details, connected devices and network layout, which helps an attacker plan their next step.

SOLUTION

1. Disable SNMPv1/v2c or change the community string to a long random value.
2. Prefer SNMPv3 with authentication and encryption, limited to your monitoring server.

SCORE

`CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`

xSPECTRE assessment for a default credential on an internal device (no single CVE).

REFERENCES

- RFC 3414 — SNMPv3 User-based Security Model
- Device vendor hardening guide

5 · REMEDIATION PLAN

What to fix first, next and later

Priorities combine severity, whether the asset faces the internet, and how much one change fixes. Hand this page to your IT team or IT provider.

Fix first

This week

- XS-01 Upgrade the web server on www.example.com
- XS-02 Close Remote Desktop to the internet; use a VPN or gateway with MFA
- XS-03 / XS-06 Upgrade OpenSSH on the VPN gateway (one change fixes both)
- XS-04 Patch or retire FS-OLD01 and disable SMBv1

Fix next

Within 30 days

- XS-05 Turn off TLS 1.0 and 1.1 on mail.example.com
- XS-08 Replace the SNMP "public" community on SW-CORE02

Fix later

Next maintenance window (within 90 days)

- XS-07 Add security headers to the customer portal
- The remaining 9 Medium and 37 Low findings, in the order shown in the vulnerability register

Essential Eight: patching evidence

Two of the ACSC Essential Eight strategies are **patch applications** and **patch operating systems**. Dated scan reports like this one help you gather evidence for them: they show which internet-facing and internal systems had missing patches or unsupported software on a given date, and later reports show what is still detected after you patch.

In this sample, XS-01, XS-03, XS-04 and XS-06 relate to patching, and XS-02 relates to multi-factor authentication and restricting administrative access. A scan report alone does not determine an Essential Eight maturity level; your assessor will also look at policies, processes and other controls.

After you fix

Once your team has made a change, scheduled rescans show what is still detected, so the next report shows whether each issue has cleared or needs another look.

6 · GLOSSARY

Terms used in this report

CVE	Common Vulnerabilities and Exposures: a public ID for a known security flaw, such as CVE-2024-6387.
CVSS	Common Vulnerability Scoring System: a 0–10 score for how severe a flaw is. This report uses CVSS v3.1 base scores.
Severity	Critical (9.0–10.0), High (7.0–8.9), Medium (4.0–6.9) or Low (0.1–3.9), taken from the CVSS score.
Perimeter	Your internet-facing systems: anything with a public IP address or public website.
Internal network	Servers, PCs, printers and network devices inside your office or data centre.
Scanner appliance	A small xSPECTRE virtual machine on your network that runs the internal Network Scans.
Network Scans	Checks of servers and devices for open services, outdated software and weak settings.
Web Scans	Checks of websites and web applications for common web weaknesses.
Security posture grade	A simple A–F grade, with a 0–100 health score, that tracks your overall position over time.
End of life (EOL)	Software the vendor no longer updates, so new security flaws are never fixed.
TLS	Transport Layer Security: the encryption that protects web and mail traffic.
RDP / SSH / SMB / SNMP	Remote Desktop, Secure Shell, Windows file sharing and network device monitoring protocols.

7 · DISCLAIMER

This is a sample report with fictional data. Example Pty Ltd, example.com, the host names, people and findings are invented for illustration. 203.0.113.0/24 is an address range reserved for documentation (RFC 5737) and 10.20.0.0/16 is a private range. The layout and content of your own reports depend on your plan, report type and scan results.

Vulnerability scanning identifies known weaknesses and risky settings at a point in time. It cannot find every issue, results can include false positives, and it does not guarantee that systems are secure or compliant with any standard or framework. Reports help you gather evidence; they are not a certification.

CVE details and scores are from the National Vulnerability Database (nvd.nist.gov) at the time of writing. Product documentation: docs.xspectre.io.