Smarttech
YOUR 24/7 SECURITY PARTNER

Oracle Solaris Third Party Bulletin – 22nd July 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	123
Authors	Dorin Constantin Banu < constatin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-07-22
Issue Date	2026-07-21

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Multiple vulnerabilities have been identified in third-party components in Oracle Solaris. Successful exploitation could result in remote code execution, privilege escalation, unauthorized access, or denial-of-service conditions.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

More details related to these vulnerabilities are as follows:

CVE ID	CVSS Score	Third Party component
CVE-2026-39821	**10**	**Go Programming Language**
CVE-2026-32792	**9.8**	**Unbound**
CVE-2026-34180	**9.8**	**OpenSSL**
CVE-2026-5731	**9.8**	**Firefox**
CVE-2026-5731	**9.8**	**Thunderbird**
CVE-2026-8388	**9.8**	**Firefox**
CVE-2026-8388	**9.8**	**Thunderbird**
CVE-2026-38974	**8.8**	**Dulwich**
CVE-2026-5402	**8.8**	**Wireshark**
CVE-2026-9759	**8.8**	**Wireshark**
CVE-2026-29518	**8.1**	**RSYNC**
CVE-2026-41316	**8.1**	**Ruby**
CVE-2026-4786	**8.1**	**Python**
CVE-2026-8643	**8**	**PIP**
CVE-2026-34000	**7.8**	**X.Org**

CVE-2026-42308	**7.8**	**Python Imaging Library (PIL)**
CVE-2026-50256	**7.8**	**X.Org**
CVE-2026-29170	**7.5**	**Apache HTTP server**
CVE-2026-33811	**7.5**	**Go Programming Language**
CVE-2026-41284	**7.5**	**Apache Tomcat**
CVE-2026-42304	**7.5**	**Twisted**
CVE-2026-44431	**7.5**	**Urllib3**
CVE-2026-46529	**7**	**Evince**
CVE-2026-6019	**6.8**	**Python**
CVE-2026-22009	**6.5**	**MySQL**
CVE-2026-8328	**6.5**	**Python**
CVE-2026-3219	**5.8**	**PIP**
CVE-2025-14179	**5.1**	**PHP**
CVE-2026-1502	**4.5**	**Python**

Affected Products

- Oracle Solaris 11.4, Oracle Solaris 11.3, and Oracle Solaris 10.

Recommendations

Smarttech247 team recommendations:

- Apply appropriate patches or appropriate mitigations provided by Oracle to vulnerable systems immediately after appropriate testing. (M1051: Update Software)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2: Establish and Maintain a Remediation Proce**ss: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.4: Perform Automated Application Patch Management**: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5 : Perform Automated Vulnerability Scans of Internal Enterprise Assets**: Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities**: Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date**: Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
    - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program**: Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program

characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2: Perform Periodic External Penetration Tests**: Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - **Safeguard 18.3: Remediate Penetration Test Findings**: Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. (M1016: Vulnerability Scanning):
    - **Safeguard 16.13: Conduct Application Penetration Testing**: Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

- Apply the Principle of Least Privilege to all systems and services and run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack. (M1026: Privileged Account Management):
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software**: Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts**: Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
    - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts**: Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- Remind all users not to visit untrusted websites or follow links/open files provided by unknown or untrusted sources. (M1017: User Training):
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program**: Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and,

at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks**: Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (M1040: Behavior Prevention on Endpoint):
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution**: Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (M1050: Exploit Protection):
    - **Safeguard 10.5: Enable Anti-Exploitation Features**: Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

References

https://www.oracle.com/security-alerts/bulletinjul2026.html

CVE

CVE-2026-39821
CVE-2026-32792
CVE-2026-34180
CVE-2026-5731
CVE-2026-8388
CVE-2026-38974
CVE-2026-5402
CVE-2026-9759
CVE-2026-29518
CVE-2026-41316
CVE-2026-4786
CVE-2026-8643
CVE-2026-34000
CVE-2026-42308
CVE-2026-50256
CVE-2026-29170
CVE-2026-33811
CVE-2026-41284
CVE-2026-42304
CVE-2026-44431
CVE-2026-46529

CVE-2026-6019
CVE-2026-22009
CVE-2026-8328
CVE-2026-3219
CVE-2025-14179
CVE-2026-1502

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com