Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Zero-Day Flaw in ScienceLogic SL1 Under Active Exploitation

Date of Publication	Admiralty Code	TA Number
October 22, 2024	A1	TA2024405

Summary

First Seen: September 24, 2024
Affected Product: ScienceLogic SL1
Impact: CVE-2024-9537 is a critical vulnerability in the ScienceLogic SL1 platform, allowing remote code execution (RCE). This flaw, linked to a third-party utility, was first exploited in an attack on Rackspace in September 2024, leading to the theft of limited monitoring data. ScienceLogic has released patches for affected versions, and organizations are urged to update immediately due to the vulnerability's CVSS score of 9.8 and its active exploitation.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-9537	ScienceLogic SL1 Unspecified Vulnerability	ScienceLogic SL1	✓	✓	✓

Vulnerability Details

#1 CVE-2024-9537 is a critical zero-day vulnerability discovered in the ScienceLogic SL1 platform, a widely used IT infrastructure monitoring tool. This vulnerability allows remote code execution (RCE), enabling attackers to execute arbitrary code on vulnerable systems, potentially leading to unauthorized access or manipulation of sensitive data.

#2 The flaw is linked to a third-party utility bundled within the SL1 platform, though the specific component has not been disclosed for security reasons. Exploitation of this vulnerability was first identified in an attack on Rackspace in September 2024, where attackers used this zero-day flaw to compromise internal monitoring systems.

#3

The breach at Rackspace highlighted the potential consequences of this vulnerability, as attackers were able to access internal web servers and steal limited monitoring data. Exposed data included customer usernames, account numbers, IP addresses, and encrypted credentials used within Rackspace's internal systems. Although Rackspace indicated that no sensitive customer configurations or hosted data were compromised, the stolen information could potentially be used in follow-up attacks, such as DDoS or further exploitation attempts.

#4

In response to the vulnerability, ScienceLogic released patches to address the flaw. Updates have been provided for versions 12.1.3, 12.2.3, 12.3.x, and later, with additional patches for older versions like 10.x and 11.x. Given the vulnerability's severity, with a CVSS score of 9.8, and the active exploitation, organizations using SL1 are strongly urged to apply patches and review their security posture. Failure to do so could leave them exposed to significant operational risks, including data breaches or service disruptions.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-9537	ScienceLogic SL1 versions prior to 12.1.3 ScienceLogic SL1 versions prior to 12.2.3 ScienceLogic SL1 versions prior to 12.3 ScienceLogic SL1 versions prior to 10.1.x ScienceLogic SL1 versions prior to 10.2.x ScienceLogic SL1 versions prior to 11.1.x ScienceLogic SL1 versions prior to 11.2.x ScienceLogic SL1 versions prior to 11.3.x	cpe:2.3:a:sciencelogic:sl1:*:*:*:*:*:*:*:*	CWE-829

Recommendations

Apply Security Patches Immediately: Organizations must apply the patches released for ScienceLogic SL1, covering versions 12.1.3+, 12.2.3+, and 12.3+. For older versions like 10.x and 11.x, make sure to follow ScienceLogic's guidance to apply appropriate updates.

Audit and Monitor Network Traffic: Conduct an immediate audit of your SL1 environment to identify any signs of compromise. Regularly monitor network logs for unusual activity, especially related to elevated privileges or external connections. This helps detect potential breaches early.

Segregate and Harden Critical Systems: Segregate SL1 from other critical systems using network segmentation and strict firewall rules. This limits an attack's ability to spread laterally and protects sensitive data from exposure. Implement ACLs to restrict unnecessary access.

Enforce Least Privilege and Strong Authentication: Ensure users accessing SL1 have only the minimum permissions required. Use multi-factor authentication (MFA) to add an extra layer of security, especially for remote access. This reduces the risk of unauthorized system access.

Rotate Credentials and Review Key Access: Rotate all credentials and API keys associated with SL1 immediately. This is critical, especially if you suspect prior compromise. Regularly reviewing key access ensures any stolen or exposed credentials do not lead to further attacks

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation
TA0010 Exfiltration	T1588.006 Vulnerabilities	T1588 Obtain Capabilities	T1588.005 Exploits
T1190 Exploit Public-Facing Application	T1068 Exploitation for Privilege Escalation	T1059 Command and Scripting Interpreter	

Patch Details

Upgrade to ScienceLogic SL1 versions 12.1.3+, 12.2.3+, and 12.3+, with remediations available for older versions down to 10.1.x, 10.2.x, 11.1.x, 11.2.x, and 11.3.x.

Links:
https://docs.sciencelogic.com/latest/Content/Web_Admin_and_Accounts/System_Administration/sys_admin_system_upgrade.htm

References

https://ogma.in/cve-2024-9537-critical-vulnerability-in-sciencelogic-sl1-and-mitigation-guide

https://x.com/ynezzor/status/1839931641172467907

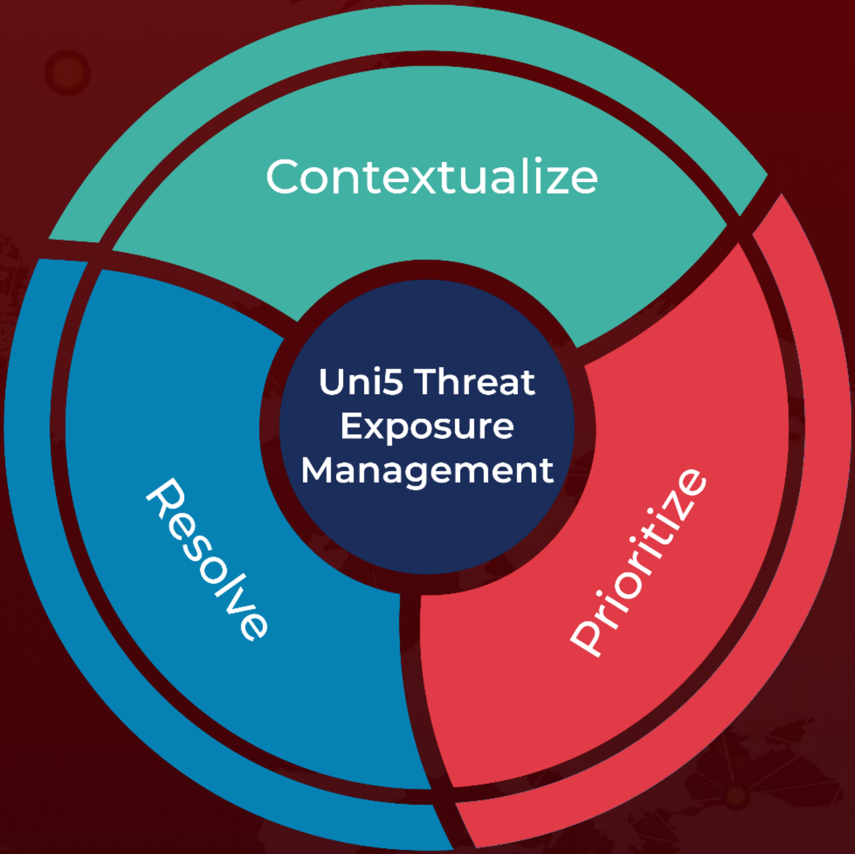
https://rackspace.service-now.com/system_status?id=detailed_status&service=4dafca5a87f41610568b206f8bbb35a6

https://www.theregister.com/2024/09/30/rackspace_zero_day_attack/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 22, 2024 • 7:30 AM

More at www.hivepro.com