Improper Handling and Insufficient Isolation of Specific Temporary Files in Splunk Enterprise

Advisory ID: SVD-2026-0403

CVE ID: CVE-2026-20204 (https://www.cve.org/CVERecord?id=CVE-2026-20204)

Published: 2026-04-15

Last Update: 2026-04-15

CVSSv3.1 Score: 7.1, High

CVSSv3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H (https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H)

CWE: CWE-377 (https://cwe.mitre.org/data/definitions/377.

Bug ID: VULN-39504

Description

In Splunk Enterprise versions below 10.2.1, 10.0.5, 9.4.10, and 9.3.11, and Splunk Cloud Platform versions below 10.4.2603.0, 10.3.2512.5, 10.2.2510.9, 10.1.2507.19, 10.0.2503.13, and 9.3.2411.127, a low-privileged user that does not hold the `admin` or `power` Splunk roles could potentially perform a Remote Code Execution (RCE) by uploading a malicious file to the `$SPLUNK_HOME/var/run/splunk/apptemp` directory due to improper handling and insufficient isolation of temporary files within the `apptemp` directory.

Solution

Upgrade Splunk Enterprise to versions 10.2.1, 10.0.5, 9.4.10, 9.3.11, or higher.

Splunk is actively monitoring and patching Splunk Cloud Platform instances.

Product Status

Product	Base Version	Component	Affected Version	Fix Version
Splunk Enterprise	10.2	Splunk Web	10.2.0	10.2.1
Splunk Enterprise	10.0	Splunk Web	10.0.0 to 10.0.4	10.0.5
Splunk Enterprise	9.4	Splunk Web	9.4.0 to 9.4.9	9.4.10
Splunk Enterprise	9.3	Splunk Web	9.3.0 to 9.3.10	9.3.11
Splunk Cloud Platform	10.4.2603	Splunk Web	Not Affected	Not Affected
Splunk Cloud Platform	10.3.2512	Splunk Web	Below 10.3.2512.5	10.3.2512.5
Splunk Cloud Platform	10.2.2510	Splunk Web	Below 10.2.2510.9	10.2.2510.9
Splunk Cloud Platform	10.1.2507	Splunk Web	Below 10.1.2507.19	10.1.2507.19
Splunk Cloud Platform	10.0.2503	Splunk Web	Below 10.0.2503.13	10.0.2503.13
Splunk Cloud Platform	9.3.2411	Splunk Web	Below 9.3.2411.127	9.3.2411.127

Mitigations and Workarounds

The vulnerability affects instances with Splunk Web turned on, turning Splunk Web off is a possible workaround. See Disable unnecessary Splunk Enterprise components (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/install-splunk-enterprise-securely/disable-unnecessary-splunk-enterprise-components) and the web.conf (https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.2/configuration-file-reference/10.2.0-configuration-file-reference/web.conf) configuration specification file for more information on turning off Splunk Web.

Detections

None

Severity

Splunk rates this vulnerability a 7.1, High, with a CVSSv3.1 vector of CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H.

Acknowledgments

Gabriel Nitu, Splunk