

CVE-2020-8496: Stored XSS in Kronos Web Time and Attendance (webTA) 4.1.x

Updated: Jan 31, 2020

Overview

This advisory addresses a Stored XSS vulnerability in Kronos Web Time and Attendance (webTA) affecting versions 4.1.x - 5.0 via the "Application Banner" input field of the "/ApplicationBanner" page.

This issue was reported to Kronos in accordance with responsible disclosure guidelines. Kronos responded that patches would be distributed by January and to include in the announcement that the latest version of Kronos webTA is not affected by this vulnerability. See screenshot of vendor email response below:

From: Kronos Security <SecurityOfficer@Kronos.com>
Sent: Tuesday, November 12, 2019 2:36 PM
To: [REDACTED]
Cc: [REDACTED] Nolan Kennedy <[REDACTED]>; Elwood Buck <[REDACTED]>
Subject: RE: Recognition for Security Vulnerabilities Discovered in Kronos WebTA

Good Afternoon [REDACTED]

Kronos is still developing patches for all affected Kronos WeTA versions, so our ask is that you wait until January (anticipated date) until we have completed generating all the patches. Additionally, our second ask is in any public statement please refer to any of the found issues as to not impact the latest release of Kronos WeTA. [REDACTED]
[REDACTED]
[REDACTED]

Thank you,

[REDACTED] | Information Security and Privacy Specialist | Kronos Incorporated
[REDACTED]

Kronos | Workforce Innovation That Works
Join Kronos on: [kronos.com](https://www.kronos.com) | [Facebook](#) | [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Kronos Email Response

Vulnerability Information

Vulnerability Categories	
CVE Identifier Description	CVE-2020-849
Vulnerability Type	Stored Cross-S
CVSSv2 score	3.6
CVSSv2 Vector String	CVSS:2.0/AV:
CVSSv3.1 Score	6.9
CVSSv3.1 Vector String	CVSS:3.1/AV:
Affected Product(s)	Kronos Web Ti
Affected Component(s)	Web Time and
Non-Affected Product(s)	Kronos Web Ti later
Who Should Read This Advisory/Apply Software Update(s)	Administrators Enterprise.

Definitions

CVE

Common Vulnerabilities and Exposures is a dictionary of common names (CVE Identifiers) for publicly known information security vulnerabilities maintained by the MITRE Corporation.

CVSS

Common Vulnerability Scoring System is a vendor agnostic, industry open standard designed to convey the severity of a vulnerability. CVSS scores may be used to determine the urgency for update deployment within an organization and can range from 0.0 (no vulnerability) to 10.0 (critical). BlackBerry uses CVSSv3 in vulnerability assessments to present an immutable characterization of security vulnerabilities. BlackBerry assigns all relevant security vulnerabilities a non-zero score. Customers performing their own risk assessments of vulnerabilities that may impact them can benefit from using the same industry-recognized CVSS metrics.

Mitigations

Mitigations are existing conditions that a potential attacker would need to overcome to mount a successful attack or that would limit the severity of an attack. Examples of such conditions include default settings, common configurations and general best practices.

Workarounds

Workarounds are settings or configuration changes that a user or administrator can apply to help protect against an attack.

Acknowledgements

This vulnerability was discovered and reported by Elwood Buck and Nolan B. Kennedy of MindPoint Group. (See email screenshot at top of page in Overview section).