hitachi-sec-2021-601 : XML Signature Wrapping Attack (XSW) issue in Hitachi ID Bravura Security Fabric

Last Update: May 29, 2021

1. Overview

Vulnerabilitiy has been fixed in Hitachi ID Bravura Security Fabric.

CVE-2021-3196: XML Signature Wrapping Attack (XSW) issue
When using federated identity management (authenticating via SAML through a third-party identity provider), an attacker injects additional data into a signed SAML response being transmitted to the service provider (Hitachi ID Bravura Security Fabric). The application successfully validates the signed values but uses the unsigned malicious values. An attacker with lower-privilege access to the application can inject the username of a high-privilege user to impersonate that user.

CVSS:2.0 AV:N/AC:L/Au:S/C:C/I:C/A:C
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE-347: Improper Verification of Cryptographic Signature

2. Affected Systems

Hitachi ID Bravura Security Fabric: 11.0.0 - 11.1.3, 12.0.0 - 12.0.2, and 12.1.0
{ "version": { "and": { "greaterThanOrEqual": "cpe:2.3:a:hitachi:hitachi_id_bravura_security_fabric:11.0.0", "lessThanOrEqual": "cpe:2.3:a:hitachi:hitachi_id_bravura_security_fabric:11.1.3" }}}
{ "version": { "and": { "greaterThanOrEqual": "cpe:2.3:a:hitachi:hitachi_id_bravura_security_fabric:12.0.0", "lessThanOrEqual": "cpe:2.3:a:hitachi:hitachi_id_bravura_security_fabric:12.0.2" }}}
cpe:2.3:a:hitachi:hitachi_id_bravura_security_fabric:12.1.0

3. Impact

Escalation of Privileges: Attackers can impersonate another user, including higher privilege levels.

4. Solution

Users and administrators are encouraged to upgrade to fixed version.

Hitachi ID Bravura Security Fabric
https://www.hitachi-id.com/products/bravura-security-fabric
CVE-2021-3196 Attackers Can Impersonate Another User
https://www.hitachi-id.com/cve-2021-3196-attackers-can-impersonate-another-user

5. References

CVE-2021-3196
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3196

6. Update history

May 29, 2021	This webpage was newly created and published.

Masato Terada (HIRT), Naoko Ohnishi (HIRT) and Michael Ellis (Hitachi Vantara)

Security Information

Related Links

Hitachi Security Advisories
Hitachi Vulnerability Disclosure Process
Acknowledgments