CAPEC-532: Altered Installed BIOS (Version 3.9)

Archived: 2026-04-05 20:35:54 UTC

CAPEC

Common Attack Pattern Enumeration and Classification

A Community Resource for Identifying and Understanding Attacks

Attack Pattern ID: 532

Abstraction: Detailed

Description

An attacker with access to download and update system software sends a maliciously altered BIOS to the victim or victim supplier/integrator, which

Likelihood Of Attack

Low

Typical Severity

High

Relationships

This table shows the other attack patterns and high level categories that are related to this attack pattern. These relationships are defined as Child(

Nature	Type
ChildOf	S Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an att

This table shows the views that this attack pattern belongs to and top level categories within that view.

View Name
Domains of Attack
Mechanisms of Attack
Supply Chain Risks

Prerequisites

Advanced knowledge about the installed target system design.
Advanced knowledge about the download and update installation processes.
Access to the download and update system(s) used to deliver BIOS images.

Skills Required

[Level: High]

Able to develop a malicious BIOS image with the original functionality as a normal BIOS image, but with added functionality that allows for later c

Mitigations

Deploy strong code integrity policies to allow only authorized apps to run.
Use endpoint detection and response solutions that can automaticalkly detect and remediate suspicious activities.
Maintain a highly secure build and update infrastructure by immediately applying security patches for OS and software, implementing mandatory
Require SSL for update channels and implement certificate transparency based verification.
Sign update packages and BIOS patches.
Use hardware security modules/trusted platform modules to verify authenticity using hardware-based cryptography.

Example Instances

An attacker compromises the download and update portion of a manufacturer's web presence, and develops a malicious BIOS that in addition to the capabilities to entice the victim to install the new BIOS quickly. The malicious BIOS is downloaded and installed on the victim's system, which allo

Taxonomy Mappings

CAPEC mappings to ATT&CK techniques leverage an inheritance model to streamline and minimize direct CAPEC/ATT&CK mappings. Inherit

Relevant to the ATT&CK taxonomy mapping

Entry ID	Entry Name
1495	Firmware Cor
1542.001	Pre-OS Boot:

References

[REF-439] John F. Miller. "Supply Chain Attack Framework and Attack Patterns". The MITRE Corporation. 2013. <http://www.mitre.org/sites/de
[REF-716] Daniel Simpson, Dani Halfin, Andrews Mariano Gorzelany and Beth Woodbury. "Supply chain attacks". Microsoft. 2021-10-28. <https

Content History

Submissions	
Submission Date	**Submitter**
2014-06-23 (Version 2.6)	CAPEC Content Team
Modifications	
Modification Date	**Modifier**
2015-11-09 (Version 2.7)	CAPEC Content Team
	Updated References, Related_Attack_Patt
2018-07-31 (Version 2.12)	CAPEC Content Team
	Updated References, Related_Attack_Patt
2019-09-30 (Version 3.2)	CAPEC Content Team
	Updated Related_Attack_Patterns
2020-07-30	CAPEC Content Team

(Version 3.3)	Updated Taxonomy_Mappings
2021-06-24 (Version 3.5)	CAPEC Content Team Updated Related_Attack_Patterns
2022-02-22 (Version 3.7)	CAPEC Content Team Updated Mitigations, References
2022-09-29 (Version 3.8)	CAPEC Content Team Updated Taxonomy_Mappings

Previous Entry Names

Change Date	**Previous Entry Name**
2015-11-09 (Version 2.7)	Altered BIOS Installed After Installation

More information is available — Please select a different filter.

Page Last Updated or Reviewed: July 31, 2018
